

# Confidentiality TOOLKIT



A resource tool from the  
ACF Interoperability Initiative

November 2021

## Confidentiality Toolkit

OPRE Report 2021-175

October 2021

Mary Gabay, Dennis Pickett, Frank Bennici, Tom Krenzke, and Janice Machado, Westat.

### Submitted to:

Brett Brown and Aaron Goldstein, Project Officers  
Office of Planning, Research, and Evaluation  
Administration for Children and Families  
U.S. Department of Health and Human Services

Contract Number: HHSP233201500671

Project Director: Janice Machado  
Westat  
1600 Research Blvd.  
Rockville, MD 20850

This report is in the public domain. Permission to reproduce is not necessary. Suggested citation: Gabay, Mary et al. (2021). Confidentiality Toolkit, OPRE Report 2021-175, Washington, DC: Office of Planning, Research, and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services.

This report and other reports sponsored by the Office of Planning, Research, and Evaluation are available at [www.acf.hhs.gov/opre](http://www.acf.hhs.gov/opre).



[Sign-up for OPRE News](#)



Follow OPRE  
on Twitter  
[@OPRE\\_ACF](https://twitter.com/OPRE_ACF)



Like OPRE's  
page on  
Facebook  
[OPRE.ACF](https://www.facebook.com/OPRE.ACF)



Follow  
OPRE on  
Instagram  
[@opre\\_acf](https://www.instagram.com/opre_acf)



Connect on  
LinkedIn  
[company/opreacf](https://www.linkedin.com/company/opreacf)



# Acknowledgements

---

The authors are grateful for the opportunity and guidance provided by the Administration for Children and Families (ACF), in particular Aaron Goldstein and Brett Brown.

An expert panel was convened in the early stages that provided important feedback throughout the course of the Toolkit update. We would like to thank all members of the Panel, and especially Bojana Bellamy and Nancy Potok, for their contributions to this document:

**Deven McGraw**  
Citizen

**Nancy Potok**  
NAPx Consulting

**Ron Prevost**  
Georgetown University,  
Massive Data Institute

**Dave Roberts**  
SEARCH Group, Inc.

**Rachel Anderson**  
Data Quality Campaign

**Bojana Bellamy**  
Centre for Information Policy Leadership at  
Hunton Andrews Kurth LLP

**Della Jenkins**  
University of Pennsylvania,  
Actionable Intelligence for Social Policy

**Sallie Ann Keller**  
Social and Decision Analytics Division,  
Biocomplexity Institute,  
University of Virginia

**Rusty Creed Brown**  
National Indian Education Association

**Ginger McCall**  
Demand Progress

We would like to thank all federal offices that contributed to this Toolkit. This includes the ACF Children's Bureau, Office of Child Care, Office of Child Support Enforcement, Office of Community Services, and Office of Family Assistance. It also includes the U.S. Department of Agriculture Food and Nutrition Service and the U.S. Department of Education Student Privacy Policy Office.

Finally, we would like to thank the individuals and organizations who contributed to the original toolkit that evolved into this publication. This includes two prior ACF employees, Joe Bodmer and Carli Wulff, and the Stewards of Change, led by Daniel Stein.

The views expressed in this publication do not necessarily reflect the views or policies of the expert panel; contributors; Office of Planning, Research, and Evaluation; ACF; or the U.S. Department of Health and Human Services.

**DISCLAIMER:** This toolkit is not official legal or regulatory guidance, and to the extent there is any conflict between this toolkit and regulations or laws, those regulations and laws take precedence.

# Preface

---

In issuing this updated Confidentiality Toolkit to support state and local data sharing efforts, we hope to bring greater clarity to the rules governing confidentiality in programs administered by the Administration for Children and Families (ACF) and certain related programs. The toolkit provides guidance, including examples, for addressing confidentiality requirements in a manner fully consistent with governing laws and underlying policies.

Human services agencies have recognized for decades that coordination and collaboration across multiple dimensions of related services can enable more effective outcomes for children, families, and individuals with multiple needs. Along with direct improvements to the delivery of services, data sharing allows federal, state, and local agencies to conduct the research and analysis needed to address existing and emerging challenges. For example, access to high quality data linked across programs and sectors will allow government agencies to develop an informed response to the devastation caused by the COVID-19 pandemic.

Many government entities have created data warehouses to support operations and/or improve the decision-making process. They have met the technological challenges associated with collecting, standardizing, linking, storing, and accessing data safely and securely. However, having the ability to securely and accurately link data across programs is not a panacea. Improved information sharing is not simply a technological challenge, but also has legal and societal constraints. Individual programs often have statutorily established confidentiality requirements to protect the privacy and dignity of individuals and families in need of assistance or services. The confidentiality provisions serve important public purposes. In some cases, confidentiality provisions may save lives, as in domestic violence programs, for example. In other cases, they are grounded in the recognition that a family in need of a particular service should not be compelled to share highly personal and private information across a full range of government agencies as a condition of receiving help.

In spite of their vital public purposes, the complexities resulting from multiple varying confidentiality provisions can be a significant impediment to state and local efforts to share data. The reconciliation of privacy requirements raises a number of questions that must be addressed, including whether a particular provision is federal, state, or local; whether it is a requirement or just a long-standing practice; whether there are exceptions; and if confidentiality can be waived through consent, how that consent can be effectuated.

We recognize that this Confidentiality Toolkit does not address all programs and every potential issue that may arise related to confidentiality and data privacy, but we hope that it will be helpful in advancing state and local efforts to improve human services delivery and outcomes through appropriate and responsible data sharing.

## **Table of Contents**

<b><u>Chapter</u></b>		<b><u>Page</u></b>
	Acknowledgements.....	iii
	Preface .....	v
1	Introduction .....	1
2	Child Welfare .....	9
3	Temporary Assistance for Needy Families (TANF).....	26
4	Child Support.....	31
5	Child Care.....	35
6	Low-Income Home Energy Assistance Program (LIHEAP).....	40
7	Supplemental Nutrition Assistance Program (SNAP) .....	43
8	Information Technology Support To Confidentiality .....	47
9	Conclusion .....	56
 <b><u>Appendixes</u></b>		
A	Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service .....	57
B	Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms.....	65
	Acronyms.....	104
	Glossary.....	106



# Chapter 1. Introduction

## The Case for Sharing

Today, persons who receive government services are often enrolled in multiple programs. A low-income parent and child may receive income assistance, food assistance, child care subsidies, health insurance, mental health care, drug or alcohol treatment services, or services from other federally supported programs. Each of these services was designed to fill a distinct purpose, with each requiring different information from individuals, and following different rules and requirements. This approach often fails to support the efficient and effective provision of services.

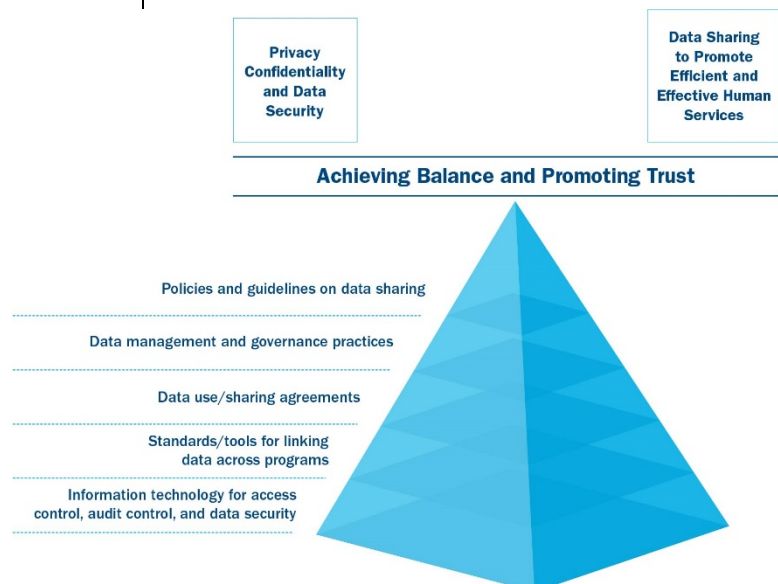
Coordinated care and integrated case management can improve the overall health and well-being of individuals. Better outcomes mean healthier, safer, more secure individuals and families who have a better chance of sustaining self-sufficiency and achieving long-term personal success. That success can, in turn, reduce costs to state and local governments.

The barriers to achieving coordination of services include confidentiality and data privacy concerns. Confidentiality and privacy have long been keystones of our society. With the advent of information technology systems, sharing

and accessing information became much easier logistically.

At the same time, legitimate concerns have arisen about data security and the potential for unauthorized sharing of personal information. Federal and state statutes and regulations designed to protect the data privacy and confidentiality rights of individuals and families sometimes make it difficult to share information across multiple programs in order to help those individuals and families.

It is increasingly important that human service providers develop balanced approaches to promote responsible information sharing. These measures must protect the confidentiality and data privacy of individuals, increase data security, improve services and outcomes, increase efficiency, and reduce duplication of efforts for both





clients and the workforce. In addition, the technological advances of the past decade provide us an opportunity to improve client outcomes and program efficiency where statutory and regulatory authority exists.

A second case for data sharing involves the tremendous potential of the research and analysis that can be conducted using linked administrative data sets. For example, an organization can integrate administrative data across multiple benefit programs into a single data warehouse and make that warehouse available to researchers and policymakers. The resulting data informed decision-making can improve agency performance and help jurisdictions craft comprehensive policy for addressing the many challenges they face. It can create confidentiality and data privacy concerns, but improved information technology and strong data governance can allay those concerns and allow for secure and accessible data.

## Purpose of the Toolkit

The Administration for Children and Families (ACF) originally developed this *Confidentiality Toolkit* in 2014 to help jurisdictions successfully navigate the balance between privacy and security with the delivery of efficient and effective services. Since that time, the relevant federal statutes and issues faced by states and localities have evolved significantly. This updated Confidentiality Toolkit reflects changes in federal law since 2014 and includes up-to-date references, agency guidance, and links

to additional resources available on the web.

The Toolkit has been developed for leaders in the human service field, to support their best efforts to share information across silos in a trusted and responsible way, taking into account confidentiality, data privacy, and security. It analyzes, explains, and aims to aid states and local jurisdictions in the navigation of a number of federal laws that impact the implementation of human services. Embedded throughout are success stories from across the country, and sample documents are provided from which jurisdictions using the Toolkit can borrow freely.

There are three distinct reasons for sharing information, all of which are essential for an effective and efficient service system:

1. Individual case planning and decision-making;
2. Informed policy making, including program development and review; and
3. Program evaluation, performance measurement, and research.

The Toolkit focuses on information sharing for the purpose of individual case planning and decision-making at a program level. Such information must be case-level and personally identifiable. Aggregated and de-identified information is useful for policy making and program development, but it is not sufficient to develop individual service plans.

This guide is also intended to help human service administrators and other professionals navigate a growing number of intersecting laws and address misconceptions about what these laws allow or do not allow. Agencies can use this Toolkit to develop data sharing procedures, using a well-reasoned, documented, and consistent approach. They can also learn how to:

- Share important information to more effectively serve clients and more efficiently allocate resources;
- Remove technical and organizational barriers to data sharing (both real and perceived); and
- Facilitate information sharing while protecting individuals' rights to confidentiality and privacy.

The Toolkit does not replace the important practice of consulting with your own legal counsel. Our aim is to outline a clear vision of what may be permissible for those interested in using data sharing to support their mission. Using this Toolkit will help enable leaders to proceed with data sharing initiatives in an organized, efficient, and consistent manner.

## Organization of the Toolkit

The Toolkit contains:

- Individual chapters addressing confidentiality and privacy through the lens of particular areas of service provision: Child Welfare, Child Support, Child Care, Temporary Assistance for Needy Families

(TANF), the Low Income Home Energy Assistance Program (LIHEAP), and the Supplemental Nutrition Assistance Program (SNAP);

- Reviews of applicable federal legislation and regulations regarding Child Welfare, Child Support, Child Care, TANF, LIHEAP, and SNAP. For each law, the Toolkit provides a basic description of the associated confidentiality issues. It highlights the law's specific language permitting information sharing when such language exists and provides specific citations for each data sharing provision;
- A discussion of how today's information technology can enable the sharing of confidential information, while ensuring data security; and



- An appendix with sample data sharing agreements,<sup>1</sup> privacy notices, and researcher data request forms from California; Montgomery County, Maryland; Indiana; and Washington.

## Individual Chapters

Individual program chapters follow the same outline addressing:

- The case for sharing, including a discussion of who benefits from shared data and how;
- The extent to which applicable federal legislation supports information sharing, including what sharing is required, what sharing is encouraged (but not required), and what actions data owners must take to protect data privacy and confidentiality;
- Practical steps and processes for successful implementation of data sharing using two workgroups – a Program Group and a Legal Group;
- A list of major federal laws and regulations; and
- A list of additional resources with links to online access.

## Getting Started

This section identifies the agency personnel and agency-level tasks that lead to trusted and responsible information sharing plans. Quality data sharing plans improve outcomes for clients, increase efficiency of operations, and protect the confidentiality and data privacy rights of individuals. Such an undertaking requires a significant investment of time and effort from cross-functional and skilled teams. It also requires leadership commitment. Necessary participants for this effort are:

- Executive leaders of each program interested in sharing data to convene groups to set the tone and direction of the effort, develop a privacy policy, and use the dictates of that policy to reach an agreement regarding the information sharing process;
- Lawyers to determine how to legally protect the confidentiality and privacy of data identified for sharing;



<sup>1</sup> This Toolkit exclusively uses the term “data sharing agreement” rather than memorandum of understanding (MOU) or memorandum of agreement (MOA) when referring to any type of agreement two or more parties enter into for the purpose of data sharing.

- IT experts to determine the most cost-effective manner of securely sharing the information;
- Security officers to implement security policies and procedures, verifying the recipients of the information and ensuring ongoing data safety;
- Disclosure avoidance experts who understand how to reduce the risk of sharing the data. Experts may be found in the statistical, mathematical, data science, or other scientific domains; and
- Program experts from the policy, operational, and practice areas to determine the specific information to be shared to achieve better outcomes for clients.

Key tasks for the agency heads leading the information sharing initiative are:

- Take the lead in the development of all data sharing agreements and cross-agency information sharing documents;
- Designate a team from the service areas that will share data to determine the **what**, or the list of minimally necessary information that needs to be shared for the legitimate governmental purpose to succeed, and the **who** that needs to receive such information;
- Designate a cross-functional team, including privacy, security, and information technology staff, to determine **how** to share the

information and protect it once shared. This group will also develop policies and procedures regarding the privacy, security, and safeguards of the shared information. The result of this process will be enforced by the privacy officials from the affected agencies;

- Arrange for training of all impacted members of the workforce on the policies and procedures for information sharing; and
- Arrange for ongoing oversight and governance of the sharing operations to sustain the benefits of sharing and maintain the public trust.

The data sharing process can be divided into three areas: policy development, staff engagement, and legal activities.

### Policy Development

Policy development answers the **why** question. Why should systems share information when they never have shared it in the past? We recommend developing two documents to provide the answer:

- A statement of “shared vision” providing the value proposition for the information sharing initiative. Information sharing that is properly executed will have benefits for all stakeholders and sectors through improved service and outcomes, enhanced customer access, and more efficient and less costly administration. This vision statement will demonstrate how stakeholders will receive value and benefit by embracing these broad outcomes,

rather than defending the status quo of “siloes” data collection and access; and

- A data sharing agreement outlining the specific purposes for information sharing, the information to be shared, how the information will be shared, and the required protections of the information once shared.

The inter-agency trust building, thought, and negotiation that is part of the process to create these documents is very important. So, while the samples included in Appendix B can be helpful in creating your own data sharing agreements, they should not be viewed as shortcuts to the real collaboration required.

Collaboration will require ongoing and consistent communication among the various agencies involved in the data sharing initiative. With separate data systems that were developed and function independently, it is likely that internal stakeholders will understand little about each other’s data systems at first. This lack of knowledge about the policies and procedures that govern another program’s system can lead to a lack of trust between staff from the various agencies that can only be overcome through sustained collaboration over time.

Building trust must be an inclusive process involving staff from different levels and roles within each agency, allowing all internal stakeholders to provide input on the importance of information sharing, the ways data

sharing could improve job performance, and the specific information required to accomplish the mission. Used inclusively, this process will build valuable agreement and agency-wide ownership. It can address common myths about how legal issues prevent data sharing and ensure internal stakeholders understand that state and federal laws allow for appropriate data sharing.



In addition to proactive, consistent internal communication, agency leadership needs to build trust with the affected client population, the legislature, providers and practitioners, other system partners, advocates, and the public. These stakeholders should be kept informed in order to address concerns that the data sharing will erode rights of confidentiality and privacy. It is the leadership’s role to communicate with external stakeholders, letting them know how the project will address data privacy and confidentiality issues and that these rights will be acknowledged and appropriately protected. External engagement in the process can ensure

that confidentiality issues are fully addressed and that there is a broad shared consensus on how best to move forward. It is also important to make clear that information technology will aid this process by securely maintaining and protecting any data involved.

Throughout, it will be important to share information on progress with all concerned constituents to ensure transparency and avoid or significantly decrease concerns about the sharing of personally identifiable information (PII).

### **Staff Engagement**

A working group of staff at all levels of the involved systems can together decide **what** information is minimally necessary to be shared for the purposes of the information sharing initiative.

This is an important and challenging part of the process because the group should be very selective and specific. If the information is not necessary for the information sharing purpose, then it should not be shared. Too little information is not useful and too much information may raise legal, confidentiality, and data privacy concerns. This group can look at examples from other jurisdictions to understand how others accomplished this task and learn about successes to follow and pitfalls to avoid.

In addition to **what** information is necessary, this group needs to determine **who** requires access to the information given the purpose. This part of the process will identify the persons or classes of persons (and the associated

supervisory chain) requiring access to the shared information and any conditions appropriate to such access. For persons or classes of persons other than case managers and their supervisory chain, this group needs to determine whether the access to shared information is necessary to perform essential functions.

Finally, all impacted employees should be trained on the new processes and procedures. Training should be considered an on-going activity to ensure new and existing employees are up-to-date on the appropriate uses of, and confidentiality protections around, shared data.

### **Legal Activities**

Agency lawyers have an integral role to play in information sharing initiatives. They provide legal and statutory interpretation, advice, and can also offer solution-oriented suggestions for accomplishing the initiative's goals. Agency leadership should communicate to their legal staff the need for and importance of the information sharing initiative, and indicate to them that the role of the lawyer is to enable this in a lawful, safe, and responsible way.

In particular, lawyers provide advice to ensure the agency complies with the law and respects individuals' rights to privacy and confidentiality. This includes review of relevant federal, state, and local laws to determine any barriers or requirements related to information sharing. For each barrier identified, the Legal Group should present suggestions,



including any legal, technical, and organizational measures that need to be implemented to overcome the barrier. The legal review process should be collaborative, solution oriented, and understandable to the layperson.

An additional task for agency lawyers is to draft appropriate privacy notices for information sharing, authorizations, and transparent policies and procedures for clients to understand that information will be shared and how it will be shared and protected. Such notices and authorizations must be understandable and inclusive of any language translations that may be required.

## **Additional Resources**

**Legal Issues for IDS Use: Finding a Way Forward. Actionable Intelligence for Social Policy, Expert Panel Report, March 2017.**

Accessed at:

<https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Legal-Issues.pdf>.



## Chapter 2. Child Welfare

---

### The Case for Sharing

Child abuse and neglect has been shown to have lifelong adverse health, social, and economic consequences for its victims. Long-term consequences for children include being at a higher risk for a wide variety of future physical health problems; lifelong psychological consequences that can manifest as educational difficulties, low self-esteem, depression, and trouble forming and maintaining relationships; and behavioral difficulties, including unhealthy sexual practices, juvenile delinquency leading to adult criminality, alcohol and other drug use, and future perpetration of maltreatment.<sup>2,3</sup>

To ensure the safety and well-being of children in foster care, all stakeholders should have current and accurate information regarding the children and their parents. Each situation is different, but the list of potential stakeholders include programs such as TANF, child support, child care, health and behavioral health, and other public benefits programs, as well as those outside of health and human services, such as education and juvenile justice. Access to current, accurate information helps ensure that appropriate services can be

delivered in a timely fashion to children in foster care. Most of the applicable child welfare statutes recognize the need for information sharing by the child welfare system with other systems and encourage or mandate that systems work together to increase successful outcomes for children and youth in foster care.

There are several different situations where the child welfare system could share information with state agencies and/or service providers to improve outcomes, increase efficiencies, and reduce redundancies. Examples include sharing data with:

- TANF/Medicaid systems, to facilitate a child's eligibility determination for title IV-E foster care maintenance payments;
- Schools, to facilitate school stability and educational improvement for children in foster care;
- Child support, to find family members to provide kinship care for a child that must be placed in out-of-home care;
- TANF, to transfer information about the child under the parent's coverage to the child welfare system;

---

<sup>2</sup> Administration for Children, Youth, and Families. Children's Bureau. Child Welfare Information Gateway Fact Sheet, Long-Term Consequences of Child Abuse and Neglect, April 2019.

<sup>3</sup> The fact sheet reports that a study by CDC using 2015 data estimated the annual cost of child maltreatment in the United States (including both tangible and intangible costs) to be \$428 billion for substantiated cases of nonfatal maltreatment.

- The juvenile justice system, to improve coordination between the child welfare case worker and the probation officer;
- The mental health system and Medicaid programs, to prevent children in foster care from receiving inappropriate psychotropic medications;
- The mental health system, to coordinate treatment for a child, their parents, or caregivers; and
- Substance use treatment systems, to access services for a child, parent, or caregiver with a substance use disorder in order to safely prevent the out-of-home placement of a child or to reunify a child.

## Applicable Federal Legislation

Included in this section is a review of some of the key provisions of federal child welfare laws and how each supports information sharing with other systems. These laws are designed to protect the rights of the children and families involved with child welfare systems. In some cases, those protections limit the dissemination of sensitive information and case-specific details. Note that there may be other federal confidentiality restrictions for the state to consider when implementing the confidentiality provisions under the laws reviewed here.

## Child Abuse Prevention and Treatment Act (CAPTA)

CAPTA is one of the key pieces of federal legislation that addresses child protection, as well as prevention and treatment of child abuse. The law includes many provisions that require or encourage information sharing and collaboration between child welfare agencies and other human service, education, justice, and health care entities. It recognizes that child welfare agencies cannot best serve children and their parents or guardians in a vacuum. There must be collaboration with others, but the confidentiality of child abuse and neglect records is paramount. The law requires that, as a condition of receiving a CAPTA state grant, a state must provide an assurance that it has in effect and is enforcing a state law that includes methods to preserve the confidentiality of all child abuse and neglect reports and records in order to protect the rights of the child and the child's parents or guardians, including requirements to ensure that the information is released only to certain individuals and entities (42 U.S.C. § 5106a(b)(2)(B)(viii)).

CAPTA includes provisions that encourage or require data sharing (presented in the first bulleted list below), specify who states *may* share data with (presented in the second bulleted list), and identify who states *must* share data with (presented in the third bulleted list). Among CAPTA's provisions that encourage or require information sharing are the following:

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• Requiring HHS to carry out a continuing interdisciplinary program of research designed to provide information needed to protect children from abuse and neglect and improve the well-being of abused and neglected children. The law provides that research programs may focus on effective approaches to interagency collaboration between the child protection system and the juvenile justice system, the medical community, providers of early childhood intervention services and special education, and domestic violence service providers;</li> <li>• Requiring HHS to provide technical assistance to states to include an evaluation or identification of effective approaches being utilized to link child protective service agencies with health care, mental health care, and developmental services;</li> <li>• Allowing HHS to provide grants to states for training to enhance linkages among child protective service agencies and health care agencies, entities providing physical and mental health services, community resources, and developmental disability agencies;</li> <li>• Allowing states to use CAPTA state grants to support and enhance interagency collaboration among public health agencies, agencies in the child protective service system, and agencies carrying out private community-based programs;</li> </ul> | <ul style="list-style-type: none"> <li>• Allowing HHS to award demonstration grants to develop a triage system that may include innovative partnerships in responding to reports of child abuse and neglect including programs of collaborative partnerships between the state child protective service agency, community social service agencies and family support programs, law enforcement agencies, developmental disability agencies, substance abuse treatment entities, health care entities, domestic violence prevention entities, mental health services, schools, churches, synagogues, and other community agencies;</li> <li>• Allowing states to use CAPTA state grants to create and improve multidisciplinary teams and interagency protocols to enhance child welfare investigations; and</li> <li>• Allowing HHS to make grants to states for the purpose of assisting child welfare agencies, social services agencies, substance use disorder treatment agencies, hospitals with labor and delivery units, medical staff, public health and mental health agencies, and maternal and child health agencies to facilitate collaboration in developing, updating, implementing, and monitoring plans of safe care for infants born and identified as being affected by substance abuse or withdrawal symptoms, or a Fetal Alcohol Spectrum Disorder. Funds</li> </ul> |
|---|--|

awarded under these grants may be used to develop and implement IT systems for improved data collection and monitoring, including existing electronic medical records, to measure the outcomes achieved through the plans of safe care.

As can be seen in the above, CAPTA does not prohibit information sharing. However, CAPTA requires that a state preserve the confidentiality of all child abuse and neglect reports and records in order to protect the rights of the child and the child's parents or guardians. These records can be released only to certain individuals and entities as authorized by state law.

The state *may* share confidential child abuse and neglect reports and records that are made and maintained in accordance with CAPTA with any of the following:

- Individuals who are the subject of a report (42 U.S.C. § 5106a(b)(2)(B)(viii)(I));
- A grand jury or court, when necessary to determine an issue before the court or grand jury (42 U.S.C. § 5106a(b)(2)(B)(viii)(V)); and
- Other entities or classes of individuals who are authorized by statute to receive information pursuant to a legitimate state purpose (42 U.S.C. § 5106a(b)(2)(B)(viii)(VI)).

In addition, states may allow public access to court proceedings that

determine child abuse and neglect cases, so long as the state can ensure the safety and well-being of the child, parents, and families involved (see the last paragraph of 42 U.S.C. § 5106a(b)(2)).

CAPTA says the state *must* provide certain otherwise confidential child abuse and neglect information to the following:

- Any federal, state, or local government entity, or any agent of such entity, that has a need for such information in order to carry out its responsibilities under law to protect children from abuse and neglect (permitted by 42 U.S.C. § 5106a(b)(2)(B)(viii)(II) but required by 42 U.S.C. § 5106a(b)(2)(B)(ix));
- Child abuse citizen review panels, if such panels are established to comply with Section 5106a(c) of CAPTA (permitted by 42 U.S.C. § 5106a(b)(2)(B)(viii)(III) but required by 42 U.S.C. § 5106a(c)(5)(A));
- Public disclosure of the findings or information about the case of child abuse or neglect that results in a child fatality or near fatality (required by 42 U.S.C. § 5106a(b)(2)(B)(x)), in accordance with Section 2.1A.4, Q/A #8 of the Children's Bureau Child Welfare Policy Manual (CWPM); and
- Child fatality review panels. Members of child fatality review panels have access to such information under 42 U.S.C. § 5106a(b)(2)(B)(viii)(IV) of CAPTA.

Authorized recipients of confidential child abuse and neglect information are bound by the same confidentiality restrictions as the child protective services agency. Thus, recipients of such information must use the information only for activities related to the prevention and treatment of child abuse and neglect. Further disclosure is permitted only in accordance with the CAPTA standards.

### **Comprehensive Child Welfare Reporting System**

The Department of Health and Human Services issued the Comprehensive Child Welfare Information System (CCWIS) Final Rule in June 2016 to address changes in technology and provide agencies with more flexibility to build smaller systems that more closely mirror their practice models. The CCWIS Final Rule encourages the implementation of information systems consistent with ACF's technology strategy of promoting program interoperability through data sharing; rapid, modular system development at lower costs; and greater efficiency through the adoption of industry standards. To receive federal financial participation, state and tribal child welfare agencies that opt to develop a CCWIS must comply with the implementing regulations at 45 C.F.R. § 1355.50-1355.59. Examples of what the agency's CCWIS must maintain include:

- Title IV-B/IV-E data that supports the efficient, effective, and economical administration of the programs including data for federal reports,

audits, reviews, and monitoring (45 C.F.R. § 1355.52(b)(1)(i) and (iv));

- The ability to support federal reporting through the Adoption and Foster Care Analysis and Reporting System (AFCARS). and for state child welfare agencies, the National Child Abuse and Neglect Data System (NCANDS) (42 U.S.C. § 674(a)(3)(C)(i) and 45 C.F.R. § 1355.52(b)(4); and
- To the extent practicable, the ability to exchange relevant data electronically with
  - Child abuse and neglect system(s);
  - System(s) operated under title IV-A of the Act (TANF);
  - Systems operated under title XIX of the Act (Medicaid);
  - Systems operated under title IV-D of the Act (child support and enforcement);
  - Systems operated by the court(s) of competent jurisdiction over title IV-E foster care, adoption, and guardianship programs; and
  - Systems operated by the state or tribal education agency, or school districts, or both. (45 C.F.R. § 1355.52(e)(2))

### **Modernizing Child Welfare Information Technology Systems**

*Child welfare practice and technology have changed considerably over time. While the State Automated Child Welfare Information System (SACWIS) regulations required a single comprehensive information system for title IV-E agencies, CCWIS allows for modular systems that provide agencies with increased flexibility to support practices that may vary within a jurisdiction. Read an overview of the CCWIS Final Rule at:*

[https://www.acf.hhs.gov/sites/default/files/documents/cb/ccwis\\_overview.pdf](https://www.acf.hhs.gov/sites/default/files/documents/cb/ccwis_overview.pdf).

### **Title IV-E of Social Security Act, Payments for Foster Care, Adoption Services, Kinship Guardianships, and Prevention Services**

Title IV-E of the Act authorizes federal reimbursement to states to provide care for children in foster family homes or child care institutions until children can safely return home, are placed permanently with adoptive or legal guardianship families, or are placed in other planned arrangements for permanency, such as independent living. Title IV-E also reimburses states and tribes for adoption assistance, and at state/tribal option, provides reimbursement for kinship guardianship assistance and time-limited prevention services for mental health, substance abuse, and in-home parent skill-based programs for children or youth who are candidates for foster care, pregnant or parenting youth in foster care, and the parents or kin caregivers of those children and youth.

States must coordinate programs under title IV-E with programs under TANF (title

IV-A of the Act), Child and Family Services (title IV-B of the Act), Social Services and Elder Justice (title XX of the Act), and other programs under appropriate federal laws.

The law states that the use or disclosure of individual information is restricted to purposes directly connected with the administration of the title IV-E plan, but permits information to be shared for numerous purposes, including the administration of certain programs and the following exceptions:

- For TANF, Child and Family Services, child support and establishment of paternity, Grants to States for Old-Age Assistance for the Aged, Maternal and Child Health Services Block Grant, Aid to the Blind, Aid to the Permanently and Totally Disabled, Supplemental Security Income (SSI), Medicaid, and Social Services;
- For criminal and civil proceedings and law enforcement in connection with the administration of one of the aforementioned programs;
- For administration of any federal or federally assisted program which provides assistance, in cash or in-kind, or services directly to individuals on the basis of need;
- For reporting and providing information to appropriate authorities with respect to known or suspected child abuse or neglect; and



### **The Family First Prevention Services Act**

*The Family First Prevention Services Act (FFPSA, 2018) contained historic reforms of the child welfare system, encouraging prevention activities designed to keep children safely with their families and ensuring children are placed in the least restrictive, most family-like setting appropriate when foster care is needed. ACF programs and state child welfare agencies are working to implement evidence-based practices around the FFPSA legislation. The Child Maltreatment Incidence Data Linkages project is an OPRE project that includes examples of innovative information sharing across sites to inform future prevention efforts. Sites link local, state, or federal administrative data, such as those from child welfare, health, social services, education, and public safety agencies, to examine the relationship between the incidence of child maltreatment and related risk and protective factors. Findings can help shape prevention and intervention efforts. Child Maltreatment Incidence Data Linkages: Project Overview. Accessed at:*

<https://www.acf.hhs.gov/opre/resource/child-maltreatment-incidence-data-linkages-project-overview>.

- For any audit or similar activity in connection with any such plan or program by any governmental agency that has authority to conduct such activity. (42 U.S.C. § 671(a)(8)).

The statute also has information sharing provisions related to education, health, special needs, qualified residential treatment program (QRTP) placement, and transition from foster care including:

- States/tribes receiving title IV-E funding must assure that each child who has attained the minimum age for compulsory school attendance under state law is a full-time elementary or secondary school student or has completed secondary school. The law also requires written education case plans for children in foster care that must include the name and address of the education provider, grade level performance, and school record;
- Educational stability requirements for children in foster care, including assurances that each placement into

foster care takes into account the appropriateness of the current educational setting and the proximity of the placement to the school in which child is enrolled when placed;

- A requirement for state child welfare agencies to collaborate with appropriate local educational agencies to ensure that a child in foster care remains in the school in which the child is enrolled at the time of each placement, or if remaining in such school is not in the best interests of the child, to provide immediate and appropriate enrollment in a new school, with all of the education records of the child provided to the new school;
- Determination of “special needs” for an applicable child under the title IV-E adoption assistance program. An applicable child is considered “special needs” if the state has determined that the child has the presence of factors such as a medical condition or physical, mental, or emotional handicaps because of which it is reasonable to



conclude that the child cannot be placed with adoptive parents without providing title IV-E adoption assistance or Medicaid under title XIX of the Act, or, the child meets all medical or disability requirements under title XVI (supplemental security income benefits (SSI)); and a reasonable but unsuccessful effort has been made to place the child without adoption assistance or medical assistance (except where it would be against the best interest of the child); and the state has determined that the child cannot or should not be returned to the home with his or her parents;

- In the case of any child who is placed in a QRTP, a qualified individual must conduct an assessment to determine the appropriateness of the child's placement in the QRTP. In conducting the assessment, the qualified individual must work with the child's family and permanency team. The team shall consist of all appropriate biological family members, relative and fictive kin of the child, as well as, as appropriate, professionals who are a resource to the family of the child, such as teachers, medical or mental health providers who have treated the child, or clergy. If the child is 14 or older, the team must also include the members of the permanency planning team that are selected by the child;

### **Hospital and Child Welfare Data Sharing**

*Cincinnati Children's Hospital Medical Center implemented an information sharing system with the Hamilton County, Ohio child welfare agency called the Integrated Data Environment to Enhance Outcomes in Custody Youth (IDENTITY). IDENTITY links two data sets with near real-time information sharing: the hospital's electronic health records and Hamilton County's child welfare database, the State Automated Child Welfare Information System (SACWIS). A case study describes the development and implementation of this data sharing initiative whose goal is to improve health care delivery for children in protective custody. Data sharing and privacy issues were addressed through a new legal agreement between the hospital and the child welfare agency that supports data sharing and through system architecture which protects privacy by varying access for different types of system users. You can read more about this case study at:*

<https://pediatrics.aappublications.org/content/pediatrics/144/2/e20190580.full.pdf>

- Written health care case plan requirements for children in foster care must include the name and address of health care provider(s), and records of a child's immunizations, known medical problems, medications and any relevant health information;
- Education and health information must be reviewed and updated and be provided to a foster care parent/provider at the time of each placement and to youth at the age of majority under state law; and
- The state/tribal child welfare agency must provide a transition plan, with assistance and direction by the

youth, for every child in foster care attaining the age of 18 years, during the 90-day period immediately prior to that birthday. Plans must include specific options on housing, health insurance, education, continuing support services, work force supports, employment services, and information about the option to execute a health care power of attorney or other similar document recognized under state law.

### **Title IV-B of the Social Security Act, Child and Family Services**

The Social Security Act provides for the coordination of services using funds under IV-B, title XX of the Act (social services), TANF, and title IV-E of the Act (foster care maintenance and adoption services).

In accordance with 45 C.F.R. § 1355.30 (p)(3) records maintained under title IV-B and IV-E of the Act are subject to the confidentiality provisions in 45 C.F.R. § 205.50. Among other things, 45 C.F.R. § 205.50 restricts the release or use of information concerning individuals receiving financial assistance under the programs governed by this provision to certain persons or agencies that require the information for specified purposes.

The authorized recipients of this information are in turn subject to the same confidentiality standards as the agencies administering those programs. To the extent that the records of the title IV-B agency contain information

regarding child abuse and neglect reports and records, such information is subject to the confidentiality requirements at Section 5106a of CAPTA. Some of the other relevant collaboration and information-sharing elements of title IV-B include:

- To the extent feasible and appropriate, the law recommends coordinating the provision of services and benefits under other federal or federally assisted programs serving the same populations;
- Develop a plan for ongoing oversight and coordination of health care services for children in foster care with other systems, including the state's Medicaid agency. This includes a coordinated strategy to identify and respond to the physical, mental, and dental health needs of children in foster care.<sup>4</sup> The plan should also include an outline of the oversight of prescription drugs, including protocols for the appropriate use and monitoring of psychotropic medication;
- The highest court in the state can apply for Court Improvement Program Funds to ensure the safety, permanence, and well-being needs of children are met in a timely and complete manner. Applications must include a description of how courts and child welfare agencies on state and local levels will collaborate and jointly plan for the collection and

---

<sup>4</sup> Plan specifications are included in 42 U.S.C. § 622(b)(15).

sharing of all relevant data and information to demonstrate how improved case tracking and analysis of child abuse and neglect cases will produce safe and timely permanency decisions;

- Under the Regional Partnership Grants (RPG) program, HHS can award grants to regional partnerships that provide integrated activities and services designed to increase the safety, permanency, and well-being of children who are in, or are at risk of, an out-of-home placement as a result of a parent's or caretaker's substance use. From 2007 through 2019, the RPG program awarded a total of 109 funded projects in 38 states. Grantees that are not tribes or tribal consortium are required to enter into collaborative agreements with the state child welfare agency and the state agency responsible for administering the substance abuse prevention and treatment block grant;
- Under title IV-B, subpart 3, HHS, in consultation with an OMB interagency work group, is required to develop regulations designating federally required data exchange standards for title IV-B/IV-E agencies that govern;
  - Information that IV-B/IV-E agencies are required under federal law to electronically exchange with another state agency; and

***Improving the Use of Psychotropic Medication among Children and Youth in Foster Care***

*The Center for Health Care Strategies led a three-year, multi-state learning and quality improvement collaborative that brought together teams from state Medicaid, child welfare, and behavioral health agencies in six states to develop and implement new approaches to the monitoring and oversight of psychotropic medication among children and adolescents in foster care.*

*In Illinois, the legal departments within the Department of Children and Family Services and the Department of Healthcare and Family Services collaborated to develop an interagency agreement that allows for cross department data sharing related to psychotropic medication, non-psychotropic medication, medical procedures, and provider and consent information. You can read more about the results of this collaborative at: [https://www.chcs.org/media/PMQIC-Profiles\\_030818.pdf](https://www.chcs.org/media/PMQIC-Profiles_030818.pdf).*

- Federal reporting and data exchanges required by federal law.

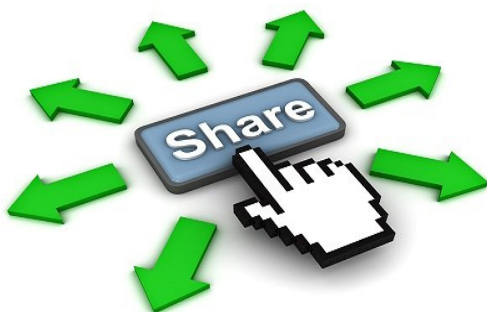
In November 2018, ACF issued a request for comments on a regulation to establish standards for data exchange between IV-B and IV-E programs, child support (title IV-D), and Temporary Assistance for Needy Families (TANF, title IV-A). A final rule has yet to be published; and

- HHS, in consultation with the Secretariat for the Interstate Compact on the Placement of Children and the States, is required to assess how the electronic interstate case-processing system

could be used to better serve and protect children that come to the attention of the child welfare system, by connecting the system with other data systems (such as systems operated by state law enforcement and judicial agencies, systems operated by the Federal Bureau of Investigation for the purposes of the Innocence Lost National Initiative, and other systems).

### **Federal Parent Locator Service**

To assist state child welfare agencies in carrying out their responsibilities, the federal Office of Child Support Enforcement (OCSE) within the U.S. Department of Health and Human Services, is required to provide state child welfare agencies with access to information contained in the Federal Parent Locator Service (42 U.S.C. § 653(j)(3)). OCSE has promulgated a rule and is partnering with the Children's Bureau and state child welfare agencies to implement this provision. OCSE and Children's Bureau Division of State Systems has provided technical assistance on the use of the Federal Parent Locator Service (FPLS) in child welfare cases through a June 2017 joint presentation. See Additional Resources.



### **Family Educational Rights and Privacy Act (FERPA) and the Uninterrupted Scholars Act (USA)**

Though not actually a child welfare-specific or other human services-related statutory authority, there are many reasons to discuss the sharing of education and academic records. Child welfare workers need accurate information about a child's education history, for example, to make informed placement recommendations to the courts. Selecting a placement that is close to the child's current school and provides the proper educational supports, including special education if necessary, is shown to improve a child's well-being, increase permanency, and help prepare older youth for successful transitions to adulthood. Sharing education records also increases transparency and accountability across different state and local agencies.

However, the child welfare program is not in charge of education records. Educational agencies and institutions (e.g., schools or school districts) that receive U.S. Department of Education funds have to comply with the Family Educational Rights and Privacy Act (FERPA), a federal statute that protects the privacy of a student's education records. The FERPA regulations are found at 34 C.F.R. Part 99. Under FERPA, the term "education records" means those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

### **Sharing Data with Courts**

*Georgia's Court Process Reporting System (CPRS) provides court stakeholders with up-to-date information about what is happening to children and parents as they move toward permanency. CPRS maintains a central repository of child records, composed of data from multiple sources, including the Department of Family and Children Service (DFCS) State Automated Child Welfare Information System (SACWIS) system from which CPRS pulls statewide foster care case plan data. CPRS integrates the information from different data sources into an easily-navigable web application for the appropriate court personnel. Court clerks can also use the system to electronically file court orders, which are then sent via a web service to DFCS, where the orders are automatically deposited into SACWIS child records. Automating this data collection dramatically reduces communication by paper documents, emails, phone calls, and office visits. You can view ACF's technical assistance guidance to courts and child welfare agencies supporting the creation of automated, bi-directional (two-way) data exchanges between their respective information systems at:*












<https://www.acf.hhs.gov/cb/training-technical-assistance/data-sharing-courts-and-child-welfare-agencies>.

FERPA generally requires that parents and eligible students (students who have reached 18 or are attending a postsecondary institution at any age) provide written consent before personally identifiable information (PII) is disclosed from the student's education records. However, FERPA has some important exceptions to its general consent requirement that would permit schools to share certain PII from education records with child welfare agencies and the courts in certain circumstances. Many educational agencies and institutions are

using these exceptions to share educational information for children in foster care among and across agencies.

For example, FERPA allows "directory information" to be disclosed without consent after the school gives general notice to all parents and eligible students of its intent to disclose directory information and the items it has designated as directory information.

Directory information can include:

-  student's name,
-  address,
-  telephone listing,
-  date of birth,
-  place of birth,
-  major field of study,
-  participation in activities and sports,
-  weight and height (for athletic teams),
-  dates of attendance,
-  degrees and awards received, and
-  the most recent educational agency attended by the student.

It is important to note, however, that a social security number or school identification number is not considered directory information for purposes of allowable disclosure without consent. Parents and eligible students also have the right to opt out of the disclosure of any or all "directory information."

It is also important to note that an educational agency or institution may not



use FERPA's directory information exception to disclose directory information combined with non-directory information. For example, a school may not use this exception to disclose a student's name, address, race, and disability status that would require consent, unless the disclosure would be consistent with another exception to FERPA's consent requirement.

The Uninterrupted Scholars Act (USA) amended the FERPA statute and became effective on January 14, 2013. The law made two very important changes to FERPA:

- USA added an additional exception to the general requirement of consent in FERPA that permits (but does not require) educational agencies and institutions to disclose education records of students in foster care placement, without parental consent, to an agency caseworker or other representative of a state or local child welfare agency or tribal organization authorized to access a student's case plan "when such agency or organization is legally responsible, in accordance with state or tribal law, for the care and protection of the student." (20 U.S.C. § 1232g(b)(1)(L)); and
- USA also amended FERPA to allow educational agencies and institutions to disclose a student's education records pursuant to a judicial order issued in specified types of judicial proceedings in which the parent is

already a party, without requiring additional notice to the parent by the educational agency or institution. (20 U.S.C. § 1232g(b)(2)(B)).

In addition to the directory information exception and the exceptions authorized by the USA, there are other important exceptions to FERPA's consent requirement. One such exception authorizes the disclosure of a student's education records when needed to comply with a judicial order or lawfully issued subpoena. Under this exception, for example, a school could disclose information from education records to any party listed on a court order, such as the child welfare agency or caseworker, caretaker, children's attorney, or court appointed special advocate.

### **Implementation: What and Who**

In most situations, sharing individually identifiable child welfare records requires permission in the form of:

- An authorization signed by a legally recognized individual;
- An individual court order mandating that information be shared; and
- A state statute mandating that individual case information be shared to better serve the client and

improve outcomes for the population, consistent with federal law.<sup>5</sup>

Regardless of how permission is obtained, a key component of any successful data sharing initiative is a written data sharing agreement that explains the information to be shared, with whom, and by what method. In some situations, a written data sharing agreement may also be required by law.<sup>6</sup>

#### **Sharing Foster Care Data with Schools**

*To help local schools identify and provide supportive educational services to foster children, the California Department of Social Services (CDSS) conducts a weekly data pull of records of youth in foster care from the Child Welfare Services Case Management System and sends the information electronically to the California Department of Education (CDE). The CDE matches the youth in the foster care list from CDSS with the students in their statewide data system, referred to as the California Longitudinal Pupil Achievement Data System, based on name, birthdate, and school of enrollment. The CDE then provides local school districts with reports identifying which of their students are in foster care.*

*You can read more about the foster youth data shared between local education agencies and child welfare agencies in California at:*




*[https://www.cdss.ca.gov/lettersnotices/entres/getinfo/acin/2016/i-77\\_16.pdf](https://www.cdss.ca.gov/lettersnotices/entres/getinfo/acin/2016/i-77_16.pdf).*

To develop that successful data sharing, states or counties should consider forming two working groups: a Program Group and a Legal Group. Since much of the direct child welfare case work is performed by private providers in some states, states should consider including representatives from the provider community on these working groups and throughout the planning process.

#### **The Program Group**

The Program Group should consist of policy and practice experts and determine **what** information to share and **who** will have access to shared information. Shared data should be limited to the minimum data necessary to conduct the proposed activities. After agreeing on a data set, the program group should determine who will have access to the data. Who has access should be based on job functions and limited to only those persons who need access in order to perform their job responsibilities.








The list of child welfare information to be shared might look something like this:

-  Name of youth,
-  Social Security Number,
-  Case Number,

<sup>5</sup> Note that under CAPTA, child welfare data can be released only as authorized under state law or state program policy. CAPTA requires states that receive child welfare funding to have a state law or program policy that maintains the confidentiality of child welfare records while authorizing access to the records for specific individuals and entities. Federal law by itself does not allow for the sharing of child welfare records.

<sup>6</sup> FERPA does not permit an educational agency or institution to disclose PII from education records pursuant to a data sharing agreement without the parent or eligible student's consent, unless permitted under an exception to FERPA's consent requirement. If one of these exceptions do apply, FERPA regulations may require the data sharing agreement to include specific provisions.



-  Participant Identification Number,
-  Current Address,
-  Contact telephone number,
-  Email address,
-  Date and place of birth,
-  Personal goals, and
-  Projected date of discharge from care.

### **The Legal Group**

The Legal Group should first decide whether the specific child welfare information is confidential and protected based on federal laws, recognizing that title IV-E/IV-B agencies may share information for purposes directly connected to the administration of specific federal programs enumerated in the law, such as TANF, Medicaid, SSI, and child support.

In addition, the Legal Group should investigate the state child welfare laws and general state privacy laws to determine if there are additional state requirements that must be met to share case information between systems. For each law, the Legal Group should suggest how to share the information and meet the requirements.

Examples of protected child welfare information may include the reasons that the child is in the custody of the state; information regarding mental health and drug and alcohol use of the child, the parent, or others involved with the family; HIV/AIDS or other communicable disease information; and, in some cases,

the circumstances of the placement and the danger to the child.

### **Implementation: How**

For protected child welfare information, there are generally three options available for information sharing: 1) written consent by the parent or guardian; 2) individual court order or subpoena; or, 3) a state statute designating a person to act for the parent/guardian. As noted above, none of these three methods is required if the information and entities are covered by a specific law which authorizes information sharing. Having said that, however, the three methods that can be employed are:

#### **1. Written Consent**

In general, the primary method for sharing a child's child welfare record information is through a written authorization or consent signed by the child (if age appropriate) and their parent.

#### **2. Court Order**

For children in foster care, there is usually a court involved. A court can order information to be shared with other systems though the confidentiality requirements enumerated in 45 C.F.R. § 205.50 do apply to the courts as well. To use this method, there must be individual, specific court orders and not a general "Order of the Court" that applies to all children.

#### **3. State Statutes**

In a number of jurisdictions, on the theory that the child welfare agency is "acting as

a parent in the absence of a parent or guardian” or “in loco parentis” for a child in the custody of the state, state law provides that once a court has entered an order of dependency, the state has the ability to release child welfare information.

## Major Federal Laws and Regulations

CAPTA; title IV-B (Child and Family Services), and title IV-E (Federal Payments for Foster Care, Adoption Services, Kinship Guardianships, and Prevention Services). Adoption and Foster Care Analysis and Reporting System Final Rule (45 C.F.R. § 1355.41); Comprehensive Child Welfare Information System Final Rule (45 C.F.R. § 1355.50); Safeguarding Information for the Financial Assistance Programs (45 C.F.R. § 205.50); and Plan Requirements for title IV-E and IV-B (45 C.F.R. § 1355.21(a)).

## Additional Resources

A Compendium of Administrative and Survey Data Resources in the Administration for Children and Families. Office of Planning, Research, and Evaluation. March 2020. Office of Family Assistance, Adoption and Foster Care Analysis and Reporting System (AFCARS), pp. 14 – 21; National Child Abuse and Neglect Data System (NCANDS), pp. 37 – 44; and National Youth in Transition Database (NYTD), pp. 53 – 59. Accessed at: <https://www.acf.hhs.gov/opre/report/compendium-administrative-and-survey-data-resources-administration-children-and->

The Children’s Bureau. Child Welfare Policy Manual, accessed at:

[https://www.acf.hhs.gov/cwpm/public\\_html/programs/cb/laws\\_policies/laws/cwpm/index.jsp](https://www.acf.hhs.gov/cwpm/public_html/programs/cb/laws_policies/laws/cwpm/index.jsp).

The Children’s Bureau. Comprehensive Child Welfare Information System. Technical Bulletin #2: Data Sharing between CCWIS and Child Welfare Contributing Agencies. Revised January 27, 2020. Accessed at: <https://www.acf.hhs.gov/cb/training-technical-assistance/ccwis-technical-bulletin-2>.

Children’s Bureau in collaboration with the Court Improvement Program, and the Child Welfare Capacity Building Center for Courts. Data Sharing: Courts and Child Welfare. 2018. Accessed at: <https://www.acf.hhs.gov/cb/training-technical-assistance/data-sharing-courts-and-child-welfare-agencies>.

ACF Information Memorandum (ACYF-CB-IM-18-02), NEW LEGISLATION – Public Law 115-123, the Family First Prevention Services Act within Division E, Title VII of the Bipartisan Budget Act of 2018. Accessed at: <https://www.acf.hhs.gov/sites/default/files/documents/cb/im1802.pdf>.

Office of Child Support Enforcement and Children’s Bureau Division of State Systems. Federal Parent Locator Service for Child Welfare Staff and Defining Automated Functions in Comprehensive Child Welfare Information Systems Presentation. June 2017. Accessed at: <https://www.acf.hhs.gov/cb/training-technical-assistance/federal-parent-locator-service-child-welfare-staff-and-defining>.

U.S. Department of Education. Guidance on the Amendments to the Family Educational Rights and Privacy Act by the Uninterrupted Scholars Act. May 2014. Accessed at: [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/uninterrupted-scholars-act-guidance.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/uninterrupted-scholars-act-guidance.pdf).

**U.S. Department of Education. Student  
Privacy Website. Accessed at:  
<https://studentprivacy.ed.gov>.**

## Chapter 3. Temporary Assistance for Needy Families (TANF)

---

### The Case for Sharing

Since replacing Aid to Families with Dependent Children (AFDC) in 1996, TANF has served as one of the nation's safety net programs for low-income families with children. TANF provides a fixed block grant of about \$16.5 billion to states, territories, and Washington, DC (hereafter referred to as "states").<sup>7</sup> Additionally, federally recognized American Indian tribes and Alaska Native organizations may elect to operate their own TANF programs. As part of the safety net for needy families, TANF is an essential partner with other systems, including child support services, SNAP, workforce development, child protective services and child welfare, Medicaid, and Unemployment Insurance.

States and tribes use their TANF funds to provide monthly cash assistance payments to low-income families with children and a wide range of services that are "reasonably calculated" to address the program's four broad purposes: (1) to provide assistance to needy families so that children may be cared for in their own homes or the homes of relatives; (2) to end the dependence of needy

parents on government benefits by promoting job preparation, work, and marriage; (3) to prevent and reduce the incidence of out-of-wedlock pregnancies; and (4) to encourage the formation and maintenance of two-parent families. ACF encourages TANF programs to work with other federal, state, and local systems to improve employment outcomes and provide comprehensive services to needy families. These systems may include education, workforce development, public housing, domestic violence and rape prevention/treatment programs, child abuse and neglect, and teenage pregnancy prevention programs.

### Applicable Federal Legislation

#### Title IV-A of the Social Security Act, Temporary Assistance for Needy Families

Under title IV-A of the Social Security Act, states have broad flexibility to implement TANF programs that best serve their distinct communities.<sup>8</sup> Within this flexibility, however, the Social Security Act requires states to "take such reasonable steps as the State deems

---

<sup>7</sup> Congressional Research Service. The Temporary Assistance for Needy Families (TANF) Block Grant: Responses to Frequently Asked Questions, Updated November 17, 2020. Accessed at: <https://fas.org/sgp/crs/misc/RL32760.pdf>.

<sup>8</sup> Section 417 of the Social Security Act limits the ability of the federal government to regulate state conduct or enforce TANF provisions, except to the extent expressly provided.

necessary to restrict the use and disclosure of information about individuals and families receiving assistance under the program...” (42 U.S.C. § 402 (a)(1)(A)(iv)). There are also a limited number of statutory requirements that speak to when and how a state may share TANF program information with other federally funded programs. For example, the Privacy Act (5 U.S.C. § 552a) permits disclosure of TANF data without an individual’s consent for a “routine use” supported by a System of Records Notice (SORN) published in the Federal Register.<sup>9</sup>

Areas where the TANF statute requires data sharing relate to eligibility determinations and child support enforcement. For example, Section 1137 of the Social Security Act (42 U.S.C § 1320b-7) requires state TANF agencies to participate in an income and eligibility verification system (IEVS). IEVS allows the state TANF agency to exchange eligibility and benefit verification information with certain other databases, including state wage data, SNAP, Medicaid, unemployment compensation benefits, and any state program administered under titles I, X, XIV (adult categories), or XVI (SSI). TANF state agencies verify SSNs by submitting them to the Social Security Administration.

Furthermore, the requirement at Sections 408(a)(2) and 408(a)(3) of the Social Security Act, and the regulations

at 45 C.F.R. § 264.30, necessitate data sharing between state TANF agencies and the relevant child support enforcement agency. These provisions require state TANF agencies to reduce cash assistance that would otherwise be available (and may eliminate it), if the child support enforcement agency determines that an individual is not cooperating in establishing paternity. State TANF agencies also must prohibit a family from receiving TANF assistance unless an assignment of support rights has been executed. A member of the family is required to assign to the state any right to support (e.g., child support) he or she may have, not exceeding the total amount of assistance paid to the family. The assignment requirement triggers the child support agency’s role to locate an absent parent, establish paternity, obtain a child support order, collect and enforce that order, and distribute and disburse the collections according to title IV-D requirements.

The TANF statute also requires state TANF agencies to provide law enforcement the current address of any cash assistance recipient in certain circumstances (42 U.S.C § 408(a)(9)(B)) and comply with general reporting requirements (42 U.S.C. § 411(a)). States are required to collect monthly, and submit quarterly, reports of individual-level data on the families receiving TANF program assistance.

---

<sup>9</sup> 5 U.S.C. § 552a (e)(4)(D). The SORN must indicate for each routine use the category of user and the purpose of such use. There are 11 routine uses for TANF program data published in the Federal Register, identifying broad categories of users and uses. (See Additional Resources.)

States may report data on all recipients or a stratified sample. Data is submitted through ACF's TANF Data Reporting System. ACF publishes aggregate data on a regular basis. Microdata is available to researchers with specific permission to access the data.

State TANF programs are authorized to request National Directory of New Hires (NDNH) data, including UI wage data, to carry out state responsibilities under the TANF program (42 U.S.C. § 653(j)(3)). The laws related to access and use of NDNH data are further discussed in Chapter 4.

Federal statutes also encourage data sharing for research purposes. TANF programs may receive NDNH data without personal identifiers to conduct research that contributes to achieving the programs' purposes (42 U.S.C. § 653 (j) (5)). Section 413 of the Social Security Act encourages research on the impact of TANF on employment, self-sufficiency, child well-being, unmarried births, marriage, poverty, economic mobility, and other factors. As required by the statute, a database has been created of projects that used "a proven approach or a promising approach in moving welfare recipients into work, based on independent, rigorous evaluations of the projects." Originally known as the "What Works Clearinghouse of Proven and Promising Projects to Move Welfare Recipients into Work," this database is now referred to as the "Pathways to Work Evidence Clearinghouse."

To further state TANF agency efforts to routinely use TANF and other administrative data to inform policy and practice, ACF sponsored the creation of the TANF Data Collaborative. The intention is to build capacity for data sharing to improve employment and well-being outcomes for individuals and families.

*The **TANF Data Collaborative (TDC)** launched in late 2017 to accelerate the use of TANF administrative data for program improvement and evidence building at the federal, state and local level.*

*TDC serves state TANF agencies through (1) targeted training and technical assistance (TTA) available to all state TANF agencies and stakeholders via the TDC TTA community and (2) the TDC Pilot Initiative, which has funded eight pilot agencies to support their efforts to build strategic partnerships for data sharing.*

*The TDC website provides access to free resources to help with the process of data acquisition, including developing agreements to share data and addressing common legal concerns and myths. The site can be accessed at: <https://www.tanfdata.org>.*

## **Implementation: What and Who**

To protect individual information while also providing efficient and coordinated services, states must make decisions based on their own laws, as well as applicable federal laws, regarding when, why, with whom, and how to share TANF information with other federally funded and assisted systems.

For successful implementation of data sharing, states or counties should consider forming two working groups: a



Program Group and a Legal Group. The state agency heads should also enter into an agreement outlining what information will be shared, with whom, and by what method. Such an agreement should consider program data needs as well as applicable state and/or federal laws. The TANF Data Collaborative (TDC) has prepared an “[MOU Inventory Checklist](#)” that lays out the information states would typically want to include in a data sharing agreement.

### **The Program Group**

The Program Group, consisting of policy and practice experts, should determine **what** information to share and **who** will have access to it. Shared data should be limited to the minimum data necessary to conduct the proposed activities. After agreeing on a limited data set, the program group should determine who will have access to the data. Who has access should be based on job functions and limited to only those persons who need access in order to perform their job responsibilities.

## **Implementation: How**

### **The Legal Group**

Since federal law and regulations do not have general prohibitions against TANF data sharing, the Legal Group should decide whether state and/or federal laws (e.g., The Privacy Act of 1974 or Section 1137 of the Social Security Act) restrict how TANF case information can be shared with other government systems. After examining applicable laws, the

group should provide suggested options for sharing the information.

Title IV-A of the Social Security Act does not require written consent from the recipient (though this may be required by state law or a court order/subpoena) for the state TANF agency to share the recipient’s information. However, the state TANF agency should (and in some cases must) provide transparency about sharing the applicant’s information with other government programs. For example, Section 1137(a)(6) of the Social Security Act requires that applicants and recipients be notified at the time of application, and periodically thereafter, that information available through the IEVS system will be requested and utilized.

## **Major Federal Laws and Regulations**

Title IV-A of the Social Security Act, Temporary Assistance for Needy Families (TANF); Section 1137 of the Social Security Act; 45 C.F.R. § 260 – 287; 45 C.F.R. § 205.50 – § 205.60.

## **Additional Resources**

Administration for Children and Families, Privacy Act of 1974; System of Records Notice. Federal Register 80:63 (April 2, 2015) p. 17904, accessed at: <https://www.govinfo.gov/content/pkg/FR-2015-04-02/pdf/2015-07440.pdf>.

TANF Data Collaborative Website, accessed at: <https://www.tanfdata.org>.



Pathways to Work Evidence Clearinghouse,  
accessed at:

<https://pathwaystowork.acf.hhs.gov>.

A Compendium of Administrative and Survey  
Data Resources in the Administration for  
Children and Families. Office of Family  
Assistance (OFA), TANF Data Reporting  
System, pp. 64 – 67, accessed at:

<https://www.acf.hhs.gov/opre/report/compendium-administrative-and-survey-data-resources-administration-children-and>.

ACF Information Memorandum (TANF-ACF-  
IM-2015-02), Data Sharing between TANF and  
Child Welfare Agencies, accessed at:

<https://www.acf.hhs.gov/ofa/policy-guidance/tanf-acf-im-2015-02-data-sharing-between-tanf-and-child-welfare-agencies>.

Administration for Children and Families,  
Office of Child Support Enforcement, A  
Guide to the National Directory of New Hires,  
April 2020, accessed at:

<https://www.acf.hhs.gov/css/training-technical-assistance/guide-national-directory-new-hires>.

## Chapter 4. Child Support

### The Case for Sharing

The federal Office of Child Support Enforcement (OCSE) collects and maintains wage, employment, and other personal data to assist state child support agencies in locating parents and enforcing child support orders. Unless otherwise specifically authorized in title IV-D of the Social Security Act (the federal child support statute), the personal information that the state's child support information system collects is confidential and cannot be shared. One reason for this clear legislative mandate is the child support system's access to very sensitive and statutorily protected information, including, but not limited to, data from the Internal Revenue Service (IRS). However, there are a number of authorized uses that allow the exchange of data with state agencies such as TANF, Foster Care, Medicaid, and SNAP.

States are required to maintain statewide automated data processing and information retrieval systems for their IV-D programs, in accordance with Section 454A of the Social Security Act. The child support statute states that the child support state agency shall have access, including automated access in the case of records maintained in automated data bases, to records of other state and local government agencies, including: vital statistics; tax and revenue records; real and titled

personal property; occupational and professional licenses; ownership and control of corporations, partnerships, and other business entities; employment security records; public assistance programs; motor vehicle department; and corrections (42 U.S.C. § 666(c)(1)(D)(i)).

#### **The Case for Sharing**

*"Our most vulnerable children, those in the child welfare system, need an extra hand to help them thrive in the face of difficult circumstances. Perhaps surprisingly to some, that extra helping hand can come from the child support community. When a new home, temporary or permanent, is needed for a child, one of the first places child welfare workers look is to other family members who might be able to care for the child.*

*Child support can be a tremendous resource for locating the child's other parent, usually the father, whose contact information may not be available from the child's mother. If the child's family has a current or former welfare case, if the parents have been divorced, if paternity has been established or if the child is on Medicaid, the child support program probably has information about the child's other parent. It is worth the time and effort for child welfare and child support agencies to build relationships and develop procedures to make sure that, when appropriate, fathers and other paternal kin have the opportunity to take responsibility for their children in need."*

*Vicki Turetsky, Commissioner, OCSE, Administration for Children and Families, Quality Improvement Center (QIC) News, National Quality Improvement Center on Non-Resident Fathers and the Child Welfare System, Quarterly Newsletter, Summer 2009, page 1.*

These automated data systems are required to be used for information comparison activities to include:

*“Exchanging information with state agencies (of the State and other States) administering programs funded under part A [TANF], programs operated under a State plan approved under title XIX [Medicaid], and other programs designated by the Secretary as necessary to perform State agency responsibilities under this part and under such programs.” – (42 U.S.C. § 654a(f)(3))*

In many instances, personally identifiable information (PII) is provided by other systems to the child support system in order to obtain a match for eligibility verification purposes.

The OCSE data system, referred to as the Federal Parent Locator Service (FPLS), includes the National Directory of New Hires (NDNH)<sup>10</sup> and the Federal Case Registry (FCR).<sup>11</sup> OCSE enters into data sharing agreements with each federal or state agency that receives FPLS information. The data sharing agreements specify the permitted purposes for sharing information, the legal authority, the information that will be compared, the specific data elements that will be disclosed, the security safeguards required for the recipient

agency to store and process NDNH data, and the expected results of the match.

## Applicable Federal Legislation

### Title IV-D of the Social Security Act, Child Support Enforcement

Title IV-D of the Social Security Act establishes standards for the establishment of paternity for children and for enforcement of child support orders for children. Title IV-D is very specific regarding the sharing of information maintained by OCSE, including the systems between which information can be shared, the specific purpose for which data can be shared, and the data elements that may be shared.

Requests for information from the FPLS must be made through a State Parent Locator Service (SPLS). Appendix A lists the persons and programs that are authorized by statute to receive information through the SPLS, the authorized purposes for which a request can be made, persons about whom information may be asked, and the specific information (including individual data elements) that can be returned to the requestor. Information cannot be shared unless specifically authorized by the statute.

<sup>10</sup> The NDNH is a database that includes information on (1) all newly hired employees, (2) the quarterly wage reports of existing employees, and (3) unemployment insurance applications and claims.

<sup>11</sup> The FCR is a national registry of child support cases and orders.

**National Database of New Hires**

*Federal law restricts access to and retention of NDNH data. ACF's A Guide to the National Directory of New Hires (April 2020) lists all authorized users of NDNH data, what information they may receive from the NDNH, and for what specific purposes.*

*Among those authorized to receive information from the NDNH are the following state agencies: TANF, child and family services, foster care, workforce agencies, and SNAP.*

*Researchers and others can obtain NDNH information but without personal identifiers.*

*Federal law requires the deletion of all NDNH data from the OCSE database after 24 months, although the Secretary of HHS may keep samples of data entered into the NDNH for research purposes.*

*ACF's A Guide to the National Directory of New Hires (April 2020) is available at:*

*<https://www.acf.hhs.gov/css/training-technical-assistance/guide-national-directory-new-hires>.*

## Implementation: What and Who

For systems to share data with the FPLS, they will have to sign a data sharing agreement with OCSE. As noted, that agreement will describe the purpose of the data sharing, the legal authority, specific data that will be matched, and the information returned to the requestor. The agreement will include a security addendum with a detailed description of the security requirements and safeguards that an agency must have in

place before receiving NDNH information from the FPLS.

## The Program Group

The Program Group, consisting of policy and practice experts from child support and other state programs legally authorized to access child support data, should follow federal law to determine what information can be shared. The law is very prescriptive regarding the specific data that can be provided from the FPLS. (See Appendix A.) The Program Group should determine who will have access to the information obtained from the FPLS, which is dependent on the policy and operational reasons for the information sharing. Access should be based on job functions and limited to those who need access to perform their job responsibilities.

## Implementation: How

### The Legal Group

Since the authority for sharing information is statutory, the issue of consent is generally not applicable. The law does not specifically block agencies from asking for consent, but obtaining consent is not required (in most instances) for agencies to seek, use, or disclose (as authorized by statute) information obtained from the FPLS.<sup>12</sup> Nor would a state court order be a proper mechanism to obtain information from

<sup>12</sup> Title IV-D of the Social Security Act makes no mention of consent except in two cases: 1) The use of FPLS data by the Department of Housing and Urban Development, and 2) The use of FPLS data by Veterans Affairs. These two agencies cannot seek, use, or disclose information from the FPLS relating to an individual without the prior written consent of the individual.

### **Helping States, Tribes, and Localities Improve their Data Sharing Capacities**

*ACF continues to invest in tools to help states, tribes, and localities improve their data sharing capacities. For example, the Children's Bureau and Office of Child Support Enforcement Joint Workgroup have created data exchange standards for case referrals from child welfare to child support agencies. The objective is to facilitate the efficient, accurate, and timely exchange of information for the establishment, enforcement, and servicing of a child support case.*

*An Information Exchange Packet Documentation was published in 2017 and can be accessed here:*

<https://www.acf.hhs.gov/completed-information-exchange-packet-documentation-iepd>.

the child support services agency if not permitted by federal law. Therefore, the lawyers for both the child support and other agencies should work together, with information technology and security personnel, to ensure that the information shared is permitted by both federal and state laws, that the purpose for the sharing is authorized, and that the information is safeguarded and maintained as required once shared.

## **Major Federal Laws and Regulations**

Title IV-D of the Social Security Act, Child Support and Establishment of Paternity, 42 § 651 – 669b; 45 C.F.R. § 300.

## **Additional Resources**

Administration for Children and Families, Office of Child Support Enforcement, A Guide to the National Directory of New Hires, April 2020. Accessed at:

[https://www.acf.hhs.gov/sites/default/files/documents/ocse/a\\_guide\\_to\\_the\\_national\\_directory\\_of\\_new\\_hires.pdf](https://www.acf.hhs.gov/sites/default/files/documents/ocse/a_guide_to_the_national_directory_of_new_hires.pdf).

A Compendium of Administrative and Survey Data Resources in the Administration for Children and Families. Office of Family Assistance, Federal Case Registry, pp. 28 – 30; National Directory of New Hires, pp. 45 – 49; and OCSE Debtor File, pp. 60 – 63.

Accessed at:

<https://www.acf.hhs.gov/opre/report/compendium-administrative-and-survey-data-resources-administration-children-and>.

## Chapter 5. Child Care

---

### The Case for Sharing

For the past 30 years, the federal government and states have promoted access to child care as a critical support for eligible low-income working families. As a result, there is important information in the eligibility records maintained by the state agencies administering child care programs under the Child Care and Development Block Grant (CCDBG) Program, also known as the Child Care and Development Fund (CCDF). In many states, enrollment for child care assistance is closely linked to other human services benefits programs, including TANF, SNAP, and Medicaid. In addition, states link child care data with information from other early care and education programs (e.g., Early Head Start, Head Start, and Pre-K) for a comprehensive view of service availability and gaps. Many states also share information from child care assistance programs with child care licensing entities and Quality Rating and Improvement Systems (QRIS) for a variety of purposes, including ensuring compliance with standards and planning technical assistance.

Unlike some other federal human services laws and regulations discussed in this Toolkit, the issues of confidentiality and information sharing are mostly absent in the federal laws and regulations related to child care. Prior to a CCDF Final Rule, published

September 30, 2016, there were no federal requirements in statute or regulation governing confidentiality in CCDF. Except as regulated by The Privacy Act of 1974, as amended, states determined the rules and practices for the sharing of information. The CCDF Final Rule requires states, territories, and tribes participating in CCDF, also referred to as lead agencies, to have policies in place to govern the use and disclosure of confidential and personally identifiable information (PII) about children and families receiving CCDF-funded assistance and child care providers. All lead agencies in the states, the District of Columbia, and the territories (hereafter referred to as “states”) were given discretion to determine the specifics of such privacy policies, provided the state’s policy complies with existing federal confidentiality requirements. The Final Rule notes that this regulatory addition was not intended to preclude the sharing of individual, case-level data among federal and state programs that can improve the delivery of services.

### Applicable Federal Legislation

#### Child Care and Development Block Grant (CCDBG)

The goal of the CCDBG Act is to help parents access safe, quality child care while employed or enrolled in training or



education. Key components of the law and federal regulations require that:

- States coordinate the provision of child care services with other federal, state, and local child care and early childhood development programs;
- States provide subsidies to eligible families to help them pay for child care;
- States give priority to children of families with very low family income and children with special needs;
- States use CCDF funds to improve the quality of child care;
- States make publicly available program-related data including provider monitoring and inspection reports, consumer education information concerning the full range of child care options analyzed by provider in order to promote informed child care choices, data and information on services for children with disabilities, and data and information on the supply of and demand for child care services in political subdivisions or regions within the state;
- States provide HHS monthly case-level reports that include sources of income (including TANF, SNAP, housing assistance) and other demographic information. Section 9858i(a)(1)(E) of the law prohibits case-level reports from containing PII;
- Eligibility criteria and priorities must promote continuity of care for children and families and may align with other human services programs (e.g., TANF, child protective services); and
- A portion of CCDF funds are used by HHS for technical assistance, and for child care research, demonstration, and evaluation activities.

The applicable regulations regarding the CCDBG Program require states to have policies in place to govern the use and disclosure of confidential information, but do not discuss specifics. The individual states decide how case information, eligibility information, and other types of case matching can be shared with other governmental units and researchers.

ACF has long encouraged states to align CCDF eligibility policies with other programs serving low-income families. In the 2014 reauthorization of the CCDBG Act, Congress established a minimum 12-month eligibility period for all children receiving child care subsidies, including children in families receiving TANF who receive CCDF-funded child care (42 U.S.C. § 9858c(c)(2)(N)(i)(I)). This longer eligibility period better aligns CCDF-funded services with other programs, such as Head Start, Early Head Start, families receiving TANF who receive SNAP, Medicaid, and the Children's Health Insurance Program (CHIP), and provides more stable child care assistance to families in need. The CCDBG Act reauthorization also offers opportunities to create greater alignment

### **The Early Childhood Data Collaborative (ECDC)**

*The ECDC supports state policymakers' development and use of coordinated state early care and education (ECE) data systems in order to provide the information needed to improve the quality of ECE programs; improve the training and quality of the early childhood workforce; increase access to high-quality ECE programs for all families; and improve child outcomes.*

*The ECDC provides technical assistance to ECE data integration projects in which sites work to integrate education, health, and social services data. Their website is accessed at:*

<https://www.childtrends.org/research-topic/ECDC>.

between CCDF and TANF-funded child care in a number of areas.<sup>13</sup> States may also match records across programs to streamline the application process for families and to promote program integrity (e.g., through verifying or documenting eligibility information).

## **Implementation: What and Who**

Given the limited data privacy and confidentiality direction provided by the child care law and regulations, the key limitations are any state laws/regulations and the federal Privacy Act of 1974, as amended.

The Privacy Act states that matching individual data between different governmental agencies is permitted if the individual consents to that activity

(5 U.S.C. § 552a(b)). The heads of the different governmental agencies should encourage the development of a data sharing agreement that details what information will be shared, when, with whom, how the information will be shared, and once shared, how the information will be maintained in a confidential manner. States should consider forming two working groups—a Program Group and a Legal Group—to help develop the details of this agreement.

The agreement is particularly important if states want to link child care with education data (including Head Start and Pre-K programs) and therefore must comply with the confidentiality and privacy requirements of the education system (i.e., the Family Educational Rights and Privacy Act, FERPA).

### **The Program Group**

The Program Group, consisting of policy and practice experts, should determine **what** information to share and **who** will have access to it. Shared data should be limited to the minimum data necessary to conduct the proposed activities. When determining data elements to be shared, it is important to note that states collect considerable case-level data. On a monthly basis, each state completes the ACF-801 form for each family receiving child care grant assistance. The ACF-801 form covers case-level data, household information (e.g., family size

<sup>13</sup> See the Information Memorandum CCDF-ACF-IM-2016-02. 2014 Child Care Reauthorization and Opportunities for TANF and CCDF. Accessed at: <https://www.acf.hhs.gov/occ/policy-guidance/child-care-reauthorization-and-opportunities-tanf-and-ccdf>.

used for eligibility purposes), income (including employment, TANF, SNAP, SSI, other federal programs and federally assisted programs), child specific information (including month/year of birth, race, and gender), and child care setting information (including data elements on the quality of care).

Each state then electronically submits a report to the Office of Child Care Information System. States have the option to report (a) on their full population or a monthly sample of about 200 facilities and (b) either monthly or quarterly. Quarterly data are due 60 days after the end of each quarter and monthly data are due 90 days after the report month. Reports submitted prior to October 2015 include personal identifiers. The reauthorization legislation prohibited PII from being included in reports starting October 2015, but they do include a unique identifier that allows for linking records on an individual across time.

After agreeing on a limited data set, the Program Group should determine who will have access to the data. Who has access should be based on job functions and limited to only those persons who need access in order to perform their job responsibilities.

## **Implementation: How**

### **The Legal Group**

The Legal Group should first consider how the information can be shared according to the Privacy Act and any state requirements. States may have

requirements which are specific to child care and/or more general privacy laws that impact child care and many other activities. Based on that analysis, the Legal Group should provide suggested options for how to share the information and meet the requirements.

Generally, the most appropriate course will be to obtain written consent from the parent or guardian to share their child's information. The Legal Group should work with the Program Group to determine how this consent should be obtained.

An authorization to share information can be drafted so that the individual "opts in," affirmatively agreeing to share child care information with the other system, or "opts out," with the notice making clear that the information will be shared unless specifically prohibited by the individual. The Legal Group should consult with the Program Group to determine the best course of action to proceed.

## **Major Federal Laws and Regulations**

Child Care and Development Block Grant, 42 U.S.C. § 9857 et seq.; The Privacy Act of 1974, 5 U.S.C. § 552a, as amended. CCDF regulations at 45 C.F.R. Part 98 and 99.

## **Additional Resources**

ACF Information Memorandum (CCDF-ACF-IM-2016-02), 2014 Child Care Reauthorization and Opportunities for TANF and CCDF.  
Accessed at:

[https://www.acf.hhs.gov/sites/default/files/documents/occ/ccdf\\_acf\\_im\\_2016\\_02.pdf](https://www.acf.hhs.gov/sites/default/files/documents/occ/ccdf_acf_im_2016_02.pdf).

Administration for Children and Families, Child Care and Development Fund (CCDF) Program, Final Rule. Federal Register 81:190 (September 30, 2016) p. 67438, accessed at: <https://www.federalregister.gov/documents/2016/09/30/2016-22986/child-care-and-development-fund-ccdf-program>.

A Compendium of Administrative and Survey Data Resources in the Administration for Children and Families. Child Care and Development Fund, Office of Child Care Information System (OCCIS), Case Level Administrative Data (ACF-801 data), pp. 22 – 27. Accessed at: <https://www.acf.hhs.gov/opre/report/compendium-administrative-and-survey-data-resources-administration-children-and>.

The Integration of Early Childhood Data. State Profiles and a Report from the U.S. Department of Health and Human Service and the U.S. Department of Education. November 2016. Accessed at: <https://www2.ed.gov/rschstat/eval/early-childhood-data/integration-early-childhood-data.pdf>.

Early Childhood Integrated Data Systems Tool Kit; Institute of Education Sciences; US Department of Education. Accessed at: <https://slds.ed.gov/#program/ecids-toolkit>.

## Chapter 6. Low-Income Home Energy Assistance Program (LIHEAP)

---

### The Case for Sharing

In many states, enrollment in LIHEAP—another critical support for low-income working families, especially those making the transition from TANF cash assistance to work—is closely linked to other human services benefits programs, including TANF, SNAP, Medicaid, and child care assistance.

The purpose of LIHEAP is to provide home energy grants, which are funded through a block grant to states, tribes, and territories (hereafter referred to as “grantees”) to meet emergency home energy needs and costs for poor and low-income persons and families. The following key components of LIHEAP indicate the intertwined nature of this federal program with other federal human services:

- Included in the definition of “emergency” is a significant enrollment increase in public benefits programs, e.g., TANF and SNAP;
- Grantees are required, in their annual application, to certify that they will only make payments under the program to households in which either 1) one or more individuals are receiving TANF, SSI, SNAP, or certain veteran’s benefits or 2) have incomes that do not exceed a specified level.;

- Programs are required to coordinate activities with similar and related programs administered by the federal or state government, particularly low-income energy-related programs administered under subtitle B of title VI (relating to the community services block grant program), under the SSI program, under TANF, under title XX of the Social Security Act, under the low-income weatherization assistance program under title IV of the Energy Conservation and Production Act, or under any other provision of law which carries out programs which were administered under the Economic Opportunity Act of 1964; and;
- For verification of income eligibility purposes, grantees may apply procedures and policies consistent with TANF or other programs.

### Applicable Federal Legislation

#### Home Energy Grants

The LIHEAP statute is codified at 42 U.S.C. § 8621-8630. Similar to the child care law, the issues of confidentiality and information sharing are not explicit in the federal law and regulations governing LIHEAP. Therefore, the key controls are the Privacy Act of 1974, as amended, and

the local laws/regulations where LIHEAP is administered.

Grantees administering the LIHEAP program are not required to report case-level data to the federal agency responsible for LIHEAP. Rather, the LIHEAP statute requires grantees to provide, as part of their annual application for the grant, the following data (42 U.S.C. § 8624 (c)(1)(G)):

- the number and income levels of households which apply for LIHEAP assistance and the number which are assisted with program funds, and
- the number of households that received assistance with one or more members who (i) had attained 60 years of age; (ii) were disabled; and (iii) were young children.

The statute also requires grantees to verify income eligibility of program participants, but does not provide explicit instructions on how this is to be done (42 U.S.C. § 8624(j)). Grantees may verify income eligibility by applying procedures consistent with procedures and policies used by the grantee agency

administering TANF or other programs specified by the statute or as determined by the state, tribe, or territory.

## Implementation: What and Who

To protect individual information, while also providing efficient and coordinated services, grantees must consider applicable local and federal laws, regarding when, why, with whom, and how to share LIHEAP information with other federally funded and assisted systems.

For successful implementation of data sharing, grantees should consider forming two working groups: a Program Group and a Legal Group. The heads of the different governmental agencies should encourage the development of a data sharing agreement outlining what information will be shared, with whom, by what method, and once shared, how the information will be maintained in a confidential manner. The Program Group and Legal Group can help develop the details of this data sharing agreement.

### The Program Group

The Program Group, consisting of policy and practice experts, should determine **what** information to share and **who** will have access to it. Shared data should be limited to the minimum data necessary to conduct the proposed activities. After agreeing on a limited data set, the Program Group should determine who will have access to the data. Who has access should be based on job functions and limited to only those persons who

#### **LIHEAP Data Used in Research**

*At the federal level, the ACF Division of Energy Assistance, Office of Community Services collects LIHEAP administrative data records from States to link them to records in the Residential Energy Consumption Survey (RECS) conducted by the U.S. Energy Information Administration. The LIHEAP data contain PII and are provided to the RECS survey contractor for research purposes. The data is not available as a public or restricted use data file. (See Additional Resources for more information).*



need access in order to perform their job responsibilities.

### **The Legal Group**

The Legal Group should consider how the information can be shared according to the Privacy Act and any local requirements which are specific to LIHEAP and/or more general privacy laws that impact LIHEAP. Based on that analysis, the Legal Group should provide suggested options for how to share the information and meet the requirements.

Generally, the most appropriate course will be to obtain the applicants'/recipients' written consent to share their information. The Legal Group should work with the Program Group to determine how this consent should be obtained.

One key question is whether the individual should be asked to “opt in” or “opt out.” Those who opt in would affirmatively agree to share LIHEAP information with other systems, while those who opt out would receive a notice making clear that their information will be shared unless specifically prohibited by the individual.

The Legal Group should determine whether a single authorization should be used by both data systems, or whether more than one is required. The Legal Group should then draft the authorization(s) and provide them to other stakeholders for comment (this often includes internal parties such as the Program Group and various external parties).

## **Major Federal Laws and Regulations**

Home Energy Grants, 42 U.S.C. § 8621;  
The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

## **Additional Resources**

**A Compendium of Administrative and Survey Data Resources in the ACF. Office of Family Assistance, Low-Income Home Energy Assistance Program (LIHEAP) Data Appended to the Residential Energy Consumption Survey (RECS), pp. 32-36.**

Accessed at:

<https://www.acf.hhs.gov/opre/report/compendium-administrative-and-survey-data-resources-administration-children-and->

## Chapter 7. Supplemental Nutrition Assistance Program (SNAP)

---

### The Case for Sharing

The Supplemental Nutrition Assistance Program (SNAP) was created to alleviate hunger and malnutrition in low-income and poor households, increase the use of the nation's available agricultural abundance, and strengthen the agricultural economy. SNAP legislation and regulations actively safeguard the personally identifiable information (PII) of applicants and recipients of SNAP benefits while permitting data sharing with a number of other public programs including:

- persons directly connected with the administration or enforcement of the SNAP program, as well as other federal assistance programs, federally assisted state programs providing assistance on a means-tested basis to low income individuals, and certain general assistance programs (7 C.F.R. § 272.1(c)(1)(i));
- programs which are required to participate in the state Income and Eligibility Verification System (IEVS) to the extent the SNAP information is useful in establishing or verifying eligibility or benefit amounts under those programs (7 C.F.R. § 272.1(c)(1)(ii));
- verification of immigration status of aliens applying for SNAP benefits,

through the Systematic Alien Verification for Entitlements (SAVE) Program (7 C.F.R. § 272.1(c)(1)(iii));

- child support enforcement programs (7 C.F.R. § 272.1(c)(1)(iv));
- local, state, or federal law enforcement officers acting in their official capacity in investigating SNAP fraud or other illegal activities (7 C.F.R. § 272.1(c)(1)(v) and (vi)); and
- local education agencies administering the National School Lunch Program (7 C.F.R. § 272.1(c)(1)(vii)).

The ability to share data across programs allows SNAP to significantly reduce the application burden on households applying for more than one public assistance program, particularly in instances where individuals may become categorically eligible for SNAP because they qualify for other assistance programs, such as TANF or SSI. For example, SNAP shares data with the National School Lunch Program to directly certify students for free or reduced price school breakfasts and lunches, relieving parents of the burden of having to complete an application.

Third-party data matches, such as matches against a state IEVS or the federal SAVE program, promote program integrity, an important program goal that

lawmakers continue to enhance with new requirements, such as establishment of the National Accuracy Clearinghouse. Improved program integrity is also supported by the computer matching program between the USDA Food and Nutrition Service (FNS) and state agencies that allows state agencies access to the Electronic Disqualified Recipient System (eDRS), a national database operated by FNS that contains records of SNAP disqualifications imposed by state agencies on individuals who have been found to have committed an intentional program violation.

## Applicable Federal Legislation

### Supplemental Nutrition Assistance Program (SNAP)

Key components of the SNAP law and federal regulations regarding information sharing include:

- State SNAP agencies must execute data exchange agreements with other agencies before exchanging information, specifying information to be exchanged and procedures used for the exchange (7 C.F.R. § 273.2(a)(4));
- A notice is required for all SNAP applications and recertifications, notifying households that information provided during the application process (including SSNs) will be verified through computer matching programs and that information may be disclosed to “other federal and state agencies for official examination, and to law enforcement

officials for the purpose of apprehending persons fleeing to avoid the law” (7 C.F.R. § 273.2(b)(4));

- The development of data exchange standards to govern “necessary categories of information that state agencies operating related programs are required under applicable law to electronically exchange with another state agency” (7 U.S.C. § 2020(v)(1));
- State agencies must establish safeguards that permit the disclosure of applicant household information to persons directly connected with the administration of other “federal assistance programs” and “federally assisted state programs” (7 U.S.C. § 2020(e)(8));
- State agencies must establish procedures for joint processing of SNAP and TANF applications (7 C.F.R. § 273.2(b)(3));
- State agencies must verify applicant employment data through the National Directory of New Hires (NDNH) for the determination of eligibility and correct benefit amounts (7 U.S.C. § 2020(e)(24));
- FNS must establish the National Accuracy Clearinghouse to prevent multiple issuances of SNAP benefits (7 U.S.C. § 2020(x)) (rulemaking has not yet been completed for this requirement);
- SNAP agencies may exchange IEVS information with agencies in other

states when the same objectives are to be met. These agencies are TANF, SNAP, Medicaid, Unemployment Compensation, and any state program administered under titles I, X, XIV (adult categories), or XVI (SSI) of the SSA. SNAP state agencies verify SSNs by submitting them to the Social Security Administration for verification (7 C.F.R. § 273.2(f)(9)); and

- Recipients of data released by the SNAP program are required to protect the data against unauthorized disclosure (7 C.F.R. § 271.1(c)(2)).

The 2018 Farm Bill also allows state agencies to establish a longitudinal database containing information about households that receive benefits under SNAP. The database must be used solely to conduct research on program participation and the operation of the SNAP program. Prior to approving the establishment of such a database, FNS must issue standards for the development of these state databases, including the way data security and privacy protections will be implemented and maintained. No PII (including social security number, home address, or contact information) may be included in those databases. FNS issued additional requirements in October 2020 and grants are expected to be awarded in late summer 2021.

## Implementation: What and Who

SNAP law and regulations require that state agencies execute a data exchange agreement that specifies the information to be exchanged and the procedures to exchange such information. Therefore, as a first step, agency heads seeking to share SNAP data should agree on a process that will lead to an executed data sharing agreement that describes the information to be shared, with whom, and by what method. The agreement should clearly state the legitimate governmental interest for the information sharing and the need to balance such interest with the interests of confidentiality and privacy. For successful implementation of data sharing, states or counties should consider forming two working groups: a Program Group and a Legal Group.

### The Program Group

The Program Group, consisting of policy and practice experts, should determine **what** information to share and **who** will have access to it. Shared data should be limited to the minimum data necessary to conduct the proposed activities. After agreeing on a limited data set, the Program Group should determine who will have access to the data. Who has access should be based on job functions and limited to only those persons who need access in order to perform their job responsibilities.

## Implementation: How

### The Legal Group

Since federal law and regulations do not have general prohibitions against SNAP data sharing, the Legal Group should decide whether state and/or federal laws (e.g., The Privacy Act of 1974 or 7 U.S.C. § 2011-2036a (Supplemental Nutrition Assistance Program)) restrict SNAP case information from being shared with other government systems for program administration or with external entities for research purposes.

The Legal Group should complete the following tasks:

- confirm that the partner agencies are among those permitted to receive SNAP data;
- review all federal and state laws that apply to information obtained by the SNAP program and partner agencies, as well as any state-specific privacy and confidentiality laws, to determine whether there are additional requirements that must be met to share case information between the partner systems. For each legal requirement, the Legal Group should provide suggested options for sharing the information and meeting the requirements. Such requirements may call for further work by the Program Group and the information technology experts; and
- draft the necessary data sharing agreement between the agencies delineating the specific information to

be shared and the procedures used to exchange and protect the shared information.

As part of its responsibilities, the Legal Group should review the required privacy notice for all SNAP applications and recertifications. To take additional steps to give notice to SNAP applicants, the privacy notice may be amended to specifically notify the applicant that SNAP shares individual household information with other state agencies, and that such information sharing is permitted by both federal and state laws.

### Major Federal Laws and Regulations

Supplemental Nutrition Assistance Program, 7 U.S.C. § 2011-2036a; 7 C.F.R. § 271-285.

### Additional Resources

Food and Nutrition Service, Supplemental Nutrition Assistance Program (SNAP) Provisions of the Agriculture Improvement Act of 2018, Information Memorandum, FNS-GD-2019-0018, March 7, 2019. Accessed at: <https://fns-prod.azureedge.net/sites/default/files/resource-files/Farm-Bill-Information-Memo.pdf>.

Request for Information: SNAP Data Exchange Standardization, USDA, May 25, 2016. Accessed at: <https://www.fns.usda.gov/snap/fr-052516>.

SNAP Longitudinal Data Project, FNS, February 17, 2021. Accessed at: <https://www.fns.usda.gov/snap/longitudinal-data-project-ldp>.

## Chapter 8. Information Technology Support To Confidentiality

---

Confidentiality is fundamentally about how we control information. It is about what information can be shared and who it can be shared with. The proper use of information technology can not only greatly increase trust between two organizations and facilitate the sharing of information; it can also greatly enhance both the security and the confidentiality of information.

Information technology enables many ways to share information. A user from one organization can be given a user ID and password to access another organization's systems. Data can be sent electronically from one system and stored in another. Data can be hosted in a secure cloud environment and accessed through a common web-based portal that draws data from multiple sources. Whatever the means of access and storage, properly designed, implemented and managed, information technology systems and procedures can facilitate the sharing, protect the confidentiality, and enhance the understanding of information.

### Enabling Information Sharing

Laws may address information sharing in a number of ways. First, information sharing may be expressly permitted (rather than prohibited) under federal or state laws. For example, SNAP and the Privacy Act of 1974, as amended, spell

out the conditions and circumstances under which SNAP case data can be used and shared. These federal laws specify the minimum thresholds of compliance. States may add additional requirements that go above and beyond these federal laws.

Second, these laws may regulate how one can be asked to consent to the sharing of personal information. This could be the individual or, in some cases, a third party like a court. For example, for children in foster care, the court can order that providers of court-ordered services provide information regarding the provision and results of such services to the court.



A common way to address specific laws regarding information sharing is to build those requirements into the information systems where the data is stored and accessed. For example, a case management system will normally be configured to restrict a caseworker's



access to only information relevant to his or her assigned cases.

Information technology systems can also electronically record an individual's positive or negative consent to share their information and then filter the information appropriately. Further, consents could be set to expire on a designated date after which data would automatically be excluded from being shared.

Systems can obtain consent through electronic and digital signatures, eliminating the need for hardcopy consent forms. An electronic signature can consist of a sound, symbol, or process that gets placed on an electronic document by a person with "intent to sign." A digital signature is a specific type of electronic signature, one that uses a certified digital ID and PIN number to prove the signer's identity.

Finally, information can be shared automatically, as in cases where a court order mandates the sharing of information. Information technology systems can record this fact and respond appropriately. For example, a system could find all of the relevant information and move it to a staging area for viewing or printing in accordance with the court order.

## Enabling Efficient Sharing

One obvious advantage of sharing data electronically is that electronic information can be viewed by more than one person at a time and, with the right tools, updated by more than one person

simultaneously with updates and changes viewable and logged in real-time by all the collaborators.

Most modern information technology environments provide a means for sharing information directly between two or more connected systems. Access may be made via a user's computer and web browser or by using an app on a mobile device such as a smartphone or tablet. Consider the example of withdrawing money from an ATM. As soon as the money is withdrawn, the transaction is reflected in the balance stored at your bank. In the same way, modern systems can be built to automatically send data based on some event or occurrence. For instance, when an elderly person becomes eligible for Medicaid services, the SNAP program could be informed to ensure the individual receives food assistance as well.

Alternatively, a public child welfare agency could provide specific access (limited as defined by the child welfare system) to a private provider of foster care services under contract with the public agency so that immediate and accurate information is shared between the agencies serving the family. The two agencies could then access each other's records, possibly via a protected web browser, and view different queries of important information and updates. Finally, systems could automatically send data to a single system where multiple users from many organizations could view that data. This concept is similar to that of a health information exchange (HIE) in which multiple

providers contribute information to a central data base that can be queried and viewed by other authorized providers.

**Montgomery County Maryland  
Enterprise Integrated Case Management  
System**

*In response to the need to improve the county's service delivery, Montgomery County Department of Health and Human Services (DHHS) officials developed an integrated case management system for County residents. The technology component of the service redesign is the enterprise integrated case management (eICM) system. In 2017, DHHS completed a three-part technology modernization initiative with the launch of its eICM. This fully integrated health and human services information system enables staff to access centralized client records, comprehensive service delivery history, and concurrent case activity information to improve outcomes of the families being served. The client-centric services include screening for all eligible services, integrated service delivery, culturally and linguistically competent services, and a focus on client and family outcomes.*

*DHHS systems represent a significant improvement in business processes, increasing service efficiency for staff by providing: comprehensive real-time views of client needs and available services; collaboration across programs and providers; immediate assessment and client referrals; improved billing practices; and cloud-based access and one-time data entry across nearly 80 programs.*

## Enabling Confidential Sharing

While this Toolkit does not examine the requirements of confidentiality and security for health information under the Health Information Portability and Accountability Act (HIPAA), the HIPAA Security Rule's (45 C.F.R. § 164) principles and guidelines are applicable

to the sharing of information where confidentiality is important. The rules set forth standards related to administrative, physical, and technical safeguards. This chapter primarily addresses the technical safeguards (45 C.F.R. § 164.312) of access control, audit control, maintaining data integrity, person or entity authentication, and encryption.

### Access Control and User Authentication

The first technical safeguard is access control (45 C.F.R. § 164.312(a)). Access control refers to the technical means used to control who can access an information technology resource. The simplest form of access control involves logging onto a computer system with account credentials and then accessing information. Access control is closely aligned with person or entity authentication (45 C.F.R. § 164.312(d)). Accessing information requires the user to first be authenticated to verify their identity, and then be authorized to access the data requested.

To authenticate a user, (i.e., verify that they are whom they say they are) the user ID assigned to an individual must be unique to that person and is typically only assigned after the person has verified his or her identity to the entity issuing the user ID. In addition to a user ID and password, additional Multifactor Authentication (MFA) items might include an ID badge with a chip that must be inserted into the user's computer, or an app to be downloaded on a smartphone and a button pressed or number read and



entered when first logging on to the system. Multifactor authentication is a substantial improvement in authentication security. It is no longer enough for an attacker to steal or guess someone's ID and password, they also need to be in physical possession of the item or device used for MFA. Before an authenticated user may access data, they must have been granted authorization to do so. This is typically done by a manager of the system and is often based on the role a user will perform.

The situation becomes more complicated when more than one organization is involved. Each organization must protect its information, but also facilitate the sharing of that information. Thus, true access control for a multi-organizational enterprise requires more robust authentication, authorization, and access control. The system should determine what resources are authorized to be accessed by a user or process and prevent resources from being accessed by unauthorized users.

In most cases, users should not be required to maintain separate sets of logon credentials to access both local and shared resources. When users must remember numerous passwords and IDs, they are more likely to take shortcuts in creating them that could leave them open to exploitation. Federated single sign-on (SSO) provides a secure, standard way to share user identities among multiple organizations. Users sign on once (the SSO) using their standard network login, typically assigned by their home organization. Their identity is then transparently and securely shared with the requested system or resource. This is what allows you to sign on to (for example) your newspaper subscription using your social media account credentials.

Use of federated SSO begins with the creation of a federation; two or more trusted partners with business and technical agreements that allow a user from one federated partner to seamlessly access resources from another partner in a secure and trustworthy manner. Such a federated approach provides a standardized means for allowing agencies to directly provide services for trusted users that they do not directly employ or manage.

Essentially, the users from one organization are trusting the credentials issued by another organization and are granting access to their resources based on that trust. This allows access decisions to be made by each participating organization in accordance

with its local policies and business practices.

For example, an attribute could define the role of the individual as a caseworker from Organization A. When this individual wishes to access information from Organization B, Organization A electronically informs Organization B that they have authenticated the individual and that the individual is a case worker. In advance, Organization B has determined and identified which information it is willing to share with caseworkers from Organization A. Using this approach, the technology not only facilitates the sharing of information between Organization A and Organization B, it also controls what information can be shared between the two and with whom.

Because mobile devices are so prevalent in today's world, organizations must plan for how access control is handled on these devices. If they are used to access or input sensitive information, they should require a PIN, password, or biometric like facial recognition before a user may gain access to the device. These devices can be made just as secure, if not more secure, than a traditional workstation or laptop, but the risk of them being lost or stolen is much greater due to their portable nature. Ensuring access control and security of the data on the device, discussed later in this chapter, will mitigate that risk. For data that is stored in an information technology system, proper use of access controls will ensure that no unauthorized person is able to access or modify data.

## **Audit Control**

Another technical safeguard called out in the HIPPA Security Rule is audit control (45 C.F.R. § 164.312(b)). Simply stated, audit control requires that organizations implement an automated means to record activity in the information system. When properly implemented, audit control will automatically keep an electronic record of everyone who creates, reads, updates, or deletes any information.

This record should contain the unique user ID and the date and time of the event. It may also record what was changed. This way, there will never be any question about the provenance of the data. In addition, automated alerts can be used to signal unauthorized attempts to access the information.

Proper use of audit controls will ensure that mistakes are detectable and traceable back to a specific individual. In addition, data can be encrypted to ensure that it will not be understandable or even readable to anyone without the proper security keys to decrypt the data.

**Integrity and Security of Data at Rest<sup>14</sup>**

The integrity (45 C.F.R. § 164.312(c)) and transmission security (45 C.F.R. § 164.312(e)) technical safeguards are related to one another in that both are intended to prevent an unauthorized party from reading or modifying information.

Maintaining the integrity of information means ensuring that it has not been changed or altered in any unauthorized way. Such alterations could happen intentionally, for example, when an individual with malicious intent tries to destroy or falsify information. It could also be through unintentional means, for example, when an employee makes a coding or transposition error while entering data. Or, it could happen through an unintended event, such as a system or media failure that causes some type of corruption in the data.

To further ensure data integrity, digital signatures may be used. When a digital signature is applied to a document, no changes can be made to that document without invalidating the signature. This ensures the reader that the final document, signed by the appropriate person or system, has not been altered.

Security of data at rest is critical to ensuring information cannot be accessed by unauthorized individuals. Most of today's applications and operating

systems provide integrated options to enable encryption of data at rest. Enabling these options, along with the access controls discussed earlier, is the most effective means of securing this type of information.

**Transmission Security**

Transmission security is intended to safeguard the electronic transmission of information, through a network, from one system to another. A secure transmission implies that no unauthorized person or intermediate system along the way was able to read or alter the data and that it reached its intended destination intact. To achieve transmission security, organizations must enable encryption. Depending on the tool, system, or process being used to transmit the data, different encryption methods should be used. For example, if the user is accessing a web application using a web browser, the web site should have an encryption certificate installed that works with the web server and web browser to encrypt the flow of information between them. In the case of a user working from a laptop at a remote location to access an organization's network resources, a Virtual Private Network (VPN) connection should be established using commonly available VPN software configured by the network administrators.

---

<sup>14</sup> Data at rest is any data that is being stored on a physical device to include a file server, database, networked folder, or mobile device such as a smartphone. It excludes data that is currently being used by a program or transferred from one location to another.

**NYC HHS CONNECT**

*HHS-Connect began as an interoperable plan to establish a client-centric approach to the service delivery systems in New York City (NYC), increase and manage the accessibility of information from one system and share it electronically with other systems, improve accountability and utilize modern and flexible technology. HHS-Connect leverages the technology resources in place at the city's Department of Information Technology and Telecommunications (DoITT). It operates two products to more efficiently and effectively provide services: ACCESS NYC and Worker Connect. ACCESS NYC is a portal for residents to explore public benefit programs, determine if they are potentially eligible, apply online, and find local help. Worker Connect is a portal to help increase the efficiency of HHS workers by providing them with an integrated view of information across HHS programs and a central point to access data from relevant HHS systems. Worker Connect links administrative case data and document vaults across multiple NYC agencies making them accessible through the single online portal. Worker Connect is a data integration system that provides access to case file data for caseworkers and managers in accordance with all applicable laws and regulations. This is made possible through:*

- *Innovative technologies that provide near real-time access to selected data and documents from multiple case management systems across NYC.*
- *A robust policy and legal framework that allows for data sharing to authorized users in accordance with all applicable laws and regulations.*
- *Granular system security to ensure Worker Connect users only see what they are legally allowed.*

These secure transmission protocols are part of most modern network infrastructures and will automatically encrypt data as it is transmitted and automatically decrypt it as it is received. This ensures that someone “eavesdropping” on the transmission would be unable to understand the contents of the transmission. In addition, most transmission protocols also ensure the integrity of the data through built-in error checking and retransmission capabilities.

## **Administrative and Physical Safeguards and Governance**

While technical security controls provide key elements of an effective security program, a complete information security program also includes administrative and

physical security considerations. Some of these controls to consider include:

- Ensuring the appropriate hosting environment for the information system. Today's technology offers many secure hosting options. A traditional in-house data center might be ideal, but hosting in a secure cloud location might offer more flexibility and options for data sharing and identity federation. If considering a cloud-based solution the key security considerations should be:
  - Does the Cloud Service Provider (CSP) meet my compliance requirements? The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program



<p>that provides a standardized approach to security and risk assessment for cloud technologies and federal agencies (<a href="https://www.fedramp.gov">fedramp.gov</a>). If federal government FISMA and NIST Risk Management Framework requirements must be met, the CSP can meet these requirement by obtaining (FedRAMP) authorization to operate.</p> <ul style="list-style-type: none"> <li>○ Does the CSP implement appropriate security for the physical, environmental, and other security controls for which they are responsible, and is there any documentation to support that?</li> <li>○ Does my organization have the IT skills to ensure that what is put in the cloud is secured appropriately? While CSPs are responsible for securing the cloud itself, the user is responsible for securing what they put in the cloud.</li> <li>• Minimizing the personally identifiable information (PII) available through data masking. Data masking is a very broad term used to describe a function applied to original data to hide real values. Several data masking protocols can be used for sharing and linking sensitive data. One example is hashing techniques that take PII (e.g., names, age,</li> </ul>	<p>gender) and converts those data fields into a single fixed length ID field.</p> <ul style="list-style-type: none"> <li>• Designating a specific individual to have primary responsibility for oversight and compliance with respect to system security. This individual can offer training and ensure all appropriate security controls are in place and working as intended throughout the system.</li> <li>• Draft and test an incident response plan to respond effectively to security incidents and potential data security breaches. This plan should detail the detection, analysis, containment, and recovery efforts if an incident occurs.</li> <li>• Scan regularly for system vulnerabilities. All systems, whether they are developed using commercial off-the-shelf (COTS) software or custom created ones, should be scanned by a vulnerability scanner on a regular schedule. The scanner will generate a report that identifies vulnerabilities that should be addressed. These vulnerabilities could be from patches that need to be applied to an operating system or default system accounts that need to have passwords updated. By quickly remediating vulnerabilities, an organization will greatly increase the security of their system.</li> <li>• Train users in information security awareness. Regular security awareness training can improve user security by making sure users of organizational information systems</li> </ul>
---	--

are aware of the security risks associated with their activities and the tools and processes the organization has available to do their job securely.

- Have a media disposal process. By establishing a standardized, systematic approach for retiring information systems and their associated physical media (e.g., disk drives, memory, and paper media) that is compliant with industry best practices as well as regulatory requirements, the organization can protect itself against accidental exposure of protected information. When media is ready for disposal, it is important to render it permanently unreadable so that anyone who might obtain the media will be unable to access the information it used to contain.

## **Additional Resources**

**Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations** accessed at:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>.

**Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology** accessed at:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.

**NIST Risk Management Framework** accessed at:

<https://csrc.nist.gov/projects/risk-management>.

## Chapter 9. Conclusion

---

The Administration for Children and Families (ACF) published the original Confidentiality Toolkit in 2014 to help jurisdictions successfully navigate the delicate balance between privacy and security and the delivery of efficient and effective services. Since the Toolkit was first published, state and local agencies have continued efforts to share data, expanding the reach of data sharing, both in terms of the number of programs included in these efforts and the government sectors (human services, education, health, and justice) involved.

While agencies consider new and better ways to share data, there is still a hesitancy in some quarters resulting from misunderstandings about what the law allows given strong privacy and confidentiality protections. Data owners are right to want to be careful, but as this Toolkit shows, federal laws authorizing public assistance programs often not only encourage data sharing, but can require it in many specific instances. Once it is understood that federal laws authorize data sharing for appropriate program administration and research purposes, program administrators, policymakers, and data users can begin to consider how to use that authority to build transparent, compliant, and accessible data sharing programs. With strong executive leadership, consultation with disclosure avoidance experts, and the collaboration of states' program, policy, legal, and information technology

teams, governance structures and information technology systems can be built and maintained to ensure the privacy and confidentiality of shared data. In addition to ensuring data security, these systems should also be transparent enough to create trust among data sharing partners, stakeholders, and program participants.

We reiterate that the Toolkit does not replace the important practice of consulting with your own legal counsel. For those interested in using data sharing to support their mission, we have outlined a clear vision of what may be permissible as you work toward the goal of sharing data to better serve those who participate in programs administered by the Administration for Children and Families (ACF) and certain related programs. Ultimately, better coordination of services can result in healthier, safer, and more secure individuals and families who will have a better chance of sustaining self-sufficiency and achieving long-term personal success, which, in turn, reduces costs to the state and local governments.

## Appendix A

### Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service

## Child Support Enforcement

---

The tables below identify the persons and programs that are authorized by statute to receive information through the State Parent Locator Service (SPLS), the authorized purposes for which a request can be made, persons about whom information may be asked, and the specific information (including individual data elements) that can be returned to the requestor.

- Most text comes from the State Parent Locator Service; Safeguarding Child Support Information; Final Rule, 73 Fed. Reg. 56422 (September 26, 2008) located at <https://www.govinfo.gov/content/pkg/FR-2008-09-26/pdf/E8-22054.pdf>.
- The text in square brackets identifies items that are not included in the tables in the Final Rule.
- Citations which say “Section” refer to the Social Security Act Title IV—Grants to States for Aid and Services to Needy Families with Children and for Child-Welfare Services located at [https://www.ssa.gov/OP\\_Home/ssact/title04/0400.htm](https://www.ssa.gov/OP_Home/ssact/title04/0400.htm).
- Please see the source text for additional information and limitations.

## Appendix A. Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service

<b>LOCATING INDIVIDUALS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)<sup>15</sup></b>				
<b>Authorized person/program</b>	<b>Authorized purpose of the request</b>	<b>Persons about whom information may be asked</b>	<b>Sources searched</b>	<b>Authorized information returned*</b>
Agent/attorney of a state [or Indian tribe or tribal organization] who has the duty or authority to collect child and spousal support under the IV-D plan. <b>Section 453(c)(1)</b>	<p>Establish paternity. Establish, set the amount, modify, or enforce child support obligations and or to facilitate the location of any individual who is under an obligation to pay child support, against whom such an obligation is sought, to whom such an obligation is owed, [or who has or may have parental rights with respect to a child]. <b>Sections 453(a)(2) and 453(a)(2)(A)(i)-(iv)</b></p> <p>Locate a parent or child involved in a non-IV-D child support case to disburse an income withholding collection. <b>Section 453(a)(2)</b></p>	<p>Noncustodial Parent Putative Father Custodial Parent Children <b>Section 453(a)(2)(A)</b></p>	<p>Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b></p> <p>In-state sources in accordance with state law.</p>	<p>Six Elements: Person's Name Person's SSN Person's address Employer's name Employer's address Employer ID Number <b>Section 453(a)(2)(A)(iii)</b></p> <p>Wages, income, and benefits of employment, including health care coverage. <b>Section 453(a)(2)(B)</b></p> <p>Type, status, location, and amount of assets or debts owed by or to the individual. <b>Section 453(a)(2)(C)</b></p>

\*See source for limitations.

<sup>15</sup> A footnote in the original table includes the following qualifiers:

- *No information shall be disclosed if the disclosure of such information would contravene the national policy or security interests of the United States or the confidentiality of census data.*
- *No information shall be disclosed if the State has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the custodial parent (CP) or child.*
- *See Section 453(b)(2) of the Act for the release process for the court or agent of the court.*



# Appendix A. Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service

LOCATING INDIVIDUALS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS) <sup>15</sup>				
Authorized person/program	Authorized purpose of the request	Persons about whom information may be asked	Sources searched	Authorized information returned*
Court that has the authority to issue an order against a non-custodial parent (NCP) for the support and maintenance of child, or to serve as the initiating court in an action to seek a child support order. <b>Section 453(c)(2)</b>	To facilitate the location of any individual who is under an obligation to pay child support, against whom such an obligation is sought, to whom such an obligation is owed, [or who has or may have parental rights with respect to a child]. <b>Section 453(a)(2)(A)(iv)</b>  Locate a parent or child involved in a non-IV-D child support case.	Noncustodial Parent Custodial Parent Putative Father Child <b>Section 453(a)(2)(A)</b>	Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b>  In-state sources in accordance with state law.	Six Elements as above. <b>Section 453(a)(2)(A)(iii)</b>  Wages, income, and benefits of employment, including health care coverage <b>Section 453(a)(2)(B)</b>  Type, status, location, and amount of assets of, or debts owed by or to the individual <b>Section 453(a)(2)(C)</b>
Resident parent, legal guardian, attorney, or agent of a child not receiving IV-A benefits (a non-IV-D request). <b>Section 453(c)(3)</b>  Tribal IV–D programs may request access to the [FPLS] under this authority.	To facilitate the location of any individual who is under an obligation to pay child support, against whom such an obligation is sought, to whom such an obligation is owed, [or who has or may have parental rights with respect to a child]. <b>Section 453(a)(2)(A)(iv)</b>  Locate a parent or child involved in a non-IV-D child support case.	Noncustodial Parent Putative Father	Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b>  In-state sources in accordance with state law.	Six Elements as above. <b>Section 453(a)(2)(A)(iii)</b>  Wages, income, and benefits of employment, including health care coverage <b>Section 453(a)(2)(B)</b>  Type, status, location, and amount of assets of, or debts owed by or to the individual <b>Section 453(a)(2)(C)</b>

\*See source for limitations.

<sup>15</sup> A footnote in the original table includes the following qualifiers:

- No information shall be disclosed if the disclosure of such information would contravene the national policy or security interests of the United States or the confidentiality of census data.
- No information shall be disclosed if the State has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the custodial parent (CP) or child.
- See Section 453(b)(2) of the Act for the release process for the court or agent of the court.

## Appendix A. Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service

<b>LOCATING INDIVIDUALS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)<sup>15</sup></b>				
<b>Authorized person/program</b>	<b>Authorized purpose of the request</b>	<b>Persons about whom information may be asked</b>	<b>Sources searched</b>	<b>Authorized information returned*</b>
State agency that is administering a Child and Family Services program (IV-B) or a Foster Care case and Adoption IV-E program. <b>Section 453(c)(4)</b>	To facilitate the location of any individual who has or may have parental rights with respect to the child. <b>Section 453(a)(2)(iv)</b>	Noncustodial Parent Putative Father Custodial Parent Child <b>Section 453(a)(2)(A)</b>	Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b>  In-state sources in accordance with state law.	Six Elements as above. <b>Section 453(a)(2)(A)(iii)</b>  Wages, income, and benefits of employment, including health care coverage <b>Section 453(a)(2)(B)</b>  Type, status, location, and amount of assets of, or debts owed by or to the individual <b>Section 453(a)(2)(C)</b>
[An entity designated as a Central Authority for child support in a foreign reciprocating country or a foreign treaty country.] <b>Section §453(c)(5)</b>	[To facilitate support enforcement in cases involving residents of the United States and residents of foreign reciprocating countries or foreign treaty countries.] <b>Section 459A(c)</b>	[Individuals sought for support enforcement purposes.] <b>Section 459A(c)(2)</b>	[Federal Parent Locator Service (FPLS).] <b>Section 459A(c)(2)</b>	[The state of residence of individuals sought for support enforcement purposes.] <b>Section 459A(c)(2)</b>

\*See source for limitations.

<sup>15</sup> A footnote in the original table includes the following qualifiers:

- *No information shall be disclosed if the disclosure of such information would contravene the national policy or security interests of the United States or the confidentiality of census data.*
- *No information shall be disclosed if the State has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the custodial parent (CP) or child.*
- *See Section 453(b)(2) of the Act for the release process for the court or agent of the court.*

<b>AUTHORITY FOR STATE IV-D AGENCIES TO RELEASE INFORMATION TO NON-IV-D FEDERAL, STATE AND TRIBAL PROGRAMS</b>				
<b>Authority</b>	<b>Authorized purpose of request</b>	<b>Authorized person/program</b>	<b>Authorized information return</b>	<b>Limitations</b>
<b>Sections 453A(h)(2) 1137 of the Act</b> – State Directory of New Hires [(SDNH)].	Eligibility verification purposes of designated programs.	State agencies administering title IV-A, Medicaid, SNAP, or other state programs under a plan approved under title I, X, XIV, or XVI of the Act.	SDNH employer-supplied information: Individual's name, address, SSN [and the date services for remuneration were first performed by the employee]; Employer's name, address, and federal employer ID number <b>Sections 453A(h)(2) and 453A(b)(1)(A)</b>	
<b>[Sections 453A(h)(3)]</b>	[For program administration.]	[State agencies operating employment security and workers' compensation programs.]	SDNH employer-supplied information: Individual's name, address, SSN [and the date services for remuneration were first performed by the employee]; Employer's name, address, and federal employer ID number <b>Sections 453A(h)(2) and 453A(b)(1)(A)</b>	
<b>[Sections 453A(h)(4)]</b>	[For the purposes of tracking employment of veterans.]	[Secretaries of Labor and Veteran Affairs.]	SDNH employer-supplied information: Individual's name, address, SSN [and the date services for remuneration were first performed by the employee]; Employer's name, address, and federal employer ID number <b>Sections 453A(h)(2) and 453A(b)(1)(A)</b>	

<b>AUTHORITY FOR STATE IV-D AGENCIES TO RELEASE INFORMATION TO NON-IV-D FEDERAL, STATE AND TRIBAL PROGRAMS</b>				
<b>Authority</b>	<b>Authorized purpose of request</b>	<b>Authorized person/program</b>	<b>Authorized information return</b>	<b>Limitations</b>
<b>Sections 453 and 454A (f)(3) of the Act, Section 1102 of the Act; and 45 C.F.R. § 307.13.</b>	To perform state or Tribal agency responsibilities of designated programs.	State or tribal agencies administering title IV, XIX, and XXI programs.	Confidential information found in automated system.	<p>No IRS information unless independently verified.  No MSFIDM [(Multistate Financial Institution Data Match)] or state FIDM information provided.  No NDNH [(National Directory of New Hires)] and FCR [(Federal Case Registry)] information for title XIX and XXI unless independently verified.</p> <p>[NDNH/FCR information may be disclosed without independent verification to title IV-D, IV-A, IV-B, and IV-E agencies.]</p> <ul style="list-style-type: none"> <li>• Need verification for other purposes.</li> </ul> <p><b>45 C.F.R. § 307.13(a)(4)(iv)</b></p>

# Appendix A. Child Support Enforcement – Authorized Disclosures from the State Parent Locator Service

LOCATING AN INDIVIDUAL SOUGHT IN A CHILD CUSTODY/VISITATION OR PARENTAL KIDNAPPING CASE <sup>15</sup>				
Authorized person/program	Authorized purpose of the request	Persons about whom info may be asked	Sources searched	Authorized information returned
<b>TYPE OF REQUEST: CHILD CUSTODY OR VISITATION CASE</b> Any agent or attorney of any state who has the authority/duty to enforce a child custody or visitation determination. <b>Section 463(d)(2)(A)</b>  A court, or agent of the court, having jurisdiction to make or enforce a child custody or visitation determination. <b>Section 463(d)(2)(B)</b>	Determining the whereabouts of a parent or child to make or enforce a custody or visitation determination. <b>Section 463(a)(2)</b>	A parent or child. <b>Section 463(a)</b>	Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b>  In-state sources in accordance with state law.	Only the three following elements: Person's Address Employer's name Employer's address <b>Section 463(c)</b>
<b>TYPE OF REQUEST: PARENTAL KIDNAPPING CASE</b> Agent or attorney of the U.S. or a state who has authority/duty to investigate, enforce, or prosecute the unlawful taking or restraint of a child. <b>Section 463(d)(2)(C)</b>	Determining the whereabouts of a parent or child to enforce any state or federal law with respect to the unlawful taking or restraint of a child. <b>Section 463(a)(1)</b>	A parent or child. <b>Section 463(a)</b>	Federal Parent Locator Service [(FPLS)]. <b>Section 453(a)(3)</b>  In-state sources in accordance with state law.	Only the three following elements: Person's Address Employer's name Employer's address <b>Section 463(c)</b>

<sup>15</sup> A footnote in the original table includes the following qualifiers:

- No information shall be disclosed if the disclosure of such information would contravene the national policy or security interests of the United States or the confidentiality of census data.
- No information shall be disclosed if the State has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the custodial parent (CP) or child.
- See Section 453(b)(2) of the Act for the release process for the court or agent of the court.

## Appendix B

Sample Data Sharing Agreements,  
Privacy Notices, and Data Request Forms



# **State of California – Memorandum of Understanding and Intra-Agency Data Exchange Agreement**

---

## **CHHS Memorandum of Understanding and Intra-Agency Data Exchange Agreement**

This Agreement sets forth a common set of terms and conditions in support of secure interoperable data exchange between and among California Health and Human Services (CHHS) Departments in compliance with all applicable federal, state and local laws, regulations and policies. The Agreement is intended to eliminate the need for CHHS Departments to enter into “point-to-point” agreements except where a different agreement is required by the federal government or federal law. You can find more information about the CHHS data sharing initiative online at: [https://chhsdata.github.io/dataplaybook/resource\\_library](https://chhsdata.github.io/dataplaybook/resource_library).

EDMUND G. BROWN JR.  
GOVERNOR

# State of California

## HEALTH AND HUMAN SERVICES AGENCY



DIANA S. DOOLEY  
SECRETARY

### CHHS Memorandum of Understanding and Intra-Agency Data Exchange Agreement

This Memorandum of Understanding and Intra-Agency Data Exchange Agreement (Agreement) is intended to facilitate data integration and exchange between departments within the California Health and Human Services Agency (CHHS) in compliance with all applicable federal, state and local laws, regulations, and policies. This Agreement is intended to be the sole agreement for data exchange among CHHS Departments and eliminates the need for CHHS Departments to enter into “point-to-point” agreements except where a different agreement is required by the federal government or federal law.

This Agreement sets forth a common set of terms and conditions in support of secure interoperable data exchange between and among CHHS Departments. The undersigned CHHS Departments have agreed to receive and/or provide data from every CHHS data source system as necessary, and have established information technology applications and infrastructure with which to share data to improve services to the citizens of California.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires a Memorandum of Understanding between governmental entities with respect to the receipt, access, use and disclosure of protected health information as defined by 45

C.F.R. § 160.103. The undersigned covered entity CHHS Departments and their business associate CHHS Departments hereby sign this Agreement to act as the Memorandum of Understanding as allowed by 45 C.F.R. § 164.504(e)(3)(i)(A).

This Agreement further sets forth the obligations of CHHS Departments that access, use, and disclose protected health information. It is understood and agreed that the Memorandum of Understanding portion of this Agreement is not intended to apply to CHHS Departments that do not meet the definition of a covered entity or business associate, as those terms are defined within 45 C.F.R. § 160.103, or the definition of hybrid entity, as that term is defined within 45 C.F.R. § 164.103, and therefore does not impose HIPAA requirements or standards on non-covered entity or non-covered components of CHHS Departments unless they are business associates of covered entity CHHS Departments.

Aging

Child Support  
Services

Community Services  
and Development

Developmental  
Services

Emergency Medical  
Services Authority

Health Care Services

Managed Health Care

Office of Patient Advocate

Office of System  
Integration

Public Health

Rehabilitation

Social Services

State Hospitals

Statewide Health  
Planning and  
Development

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

The undersigned CHHS Departments recognize that many Californians qualify for and participate in multiple State programs. Leveraging advances in technology will break down information silos within CHHS Departments and provide the following benefits:

- Assure the privacy and security of data
- Improve consumer outcomes
- Increase reliability of data
- Reduce duplication of consumer data
- Improve integration of consumer services
- Promote a consumer-centric approach to service delivery
- Improve accessibility and management of information
- Improve program effectiveness, performance, and accountability

### I. DEFINITIONS/DEFINED TERMS

- a. Authentication. Authentication is the process by which a user accessing a system demonstrates that (s)he is in fact a person or entity that is associated with an identity previously registered in the system. Authentication does not apply solely to users; it can also be applied at the system or service level (for example, by user group, department) and can be used to identify one system or service to another. It includes verifying the identity of a user, process, or device, as a prerequisite to allowing access to resources in an information system.
- b. Authorization or Authorize. The act of granting a user, program, process, or device access to data after proper identification and authentication are obtained.
- c. Authorized User. The term Authorized User is used to identify individuals approved and designated to access a CHHS data source system. Authorized Users receive rights to access a CHHS data source system from their individual CHHS Department which is solely responsible for the provisioning and de-provisioning of its employees, agents, contractors, and business associates. In granting access, such CHHS Department affirms such individuals are authorized to access the particular type and quantity of information based upon their functions and responsibilities consistent with their undisputed or approved business use cases.
- d. Business Use Case. A business use case includes a description of the functions and responsibilities of a CHHS Department or division and/or unit of a CHHS Department, the information requested, and the purpose and intended use of the information. A business use case may include, but is not limited to: (i) a brief description of each user group's business function within its department, including key roles and responsibilities of staff; (ii) individual scenarios describing how staff would make use of the data within their current business processes (such as how workers currently access these data, if applicable, and the manner in which the data are currently used); (iii) the purpose for which the data

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

would be used; and (iv) a description of the added value and benefit of accessing the requested data. Each use case also includes an associated list of relevant data sources, data categories, and/or documents supporting use case scenarios.

- e. Business Use Case Proposal. Proposal of a business use case submitted for review and approval by a Data Recipient and/or Data Provider prior to transmission of data. Business Use Case Proposals that are objected to by a Data Provider are disputed and must be reviewed and approved prior to transmission or receipt of any data by a CHHS Department unless the transfer or receipt of data is required by law or in the event the data are essential for a CHHS Department to comply with the law. Review and approval shall be completed by the Risk Management Subcommittee. The Risk Management Subcommittee shall attempt to mediate the dispute between the Data Provider and Data Recipient. If it appears to the Risk Management Subcommittee that no compromise can be reached between the disputing CHHS Departments, then the CHHS Agency Information Officer and the CHHS General Counsel will elevate the disputed Business Use Case Proposal to the Undersecretary for final decision. Business Use Case Proposals must be created for every transmission of data, including disclosures that are required by law, for tracking and auditing purposes. (See Section III, Terms and Conditions)
- f. Certification. Certification is written affirmation by a Data Recipient and/or Data Provider that its data protections meet the requirements in federal and state law, regulations, and policy, including the State Administration Manual, Chapter 5300.
- g. CHHS Departments. Referred to collectively as the departments and offices within and including the California Health and Human Services Agency as defined by California Government Code § 12803.
- h. CHHS Risk Management Subcommittee. The Risk Management Subcommittee serves as the main decision making body responsible for assessing the strategic relevance, business value, and potential liability of Business Use Case Proposals. The Risk Management Subcommittee's composition shall be determined and modified as needed by the Undersecretary. The Risk Management Subcommittee receives disputed Business Use Case Proposals from the Governance Liaison. The Risk Management Subcommittee shall approve, modify, or deny a disputed Business Use Case Proposal and explain why. The Risk Management Subcommittee shall refer a disputed Business Use Case Proposal to the Governance Liaison for review by other Governance Subcommittees when appropriate. The Governance Liaison shall collect and submit comments and recommendation on disputed Business Use Case Proposals from other Governance Advisory Subcommittees and provide them to the Risk Management Subcommittee for consideration. The Risk Management Subcommittee may seek and gather additional information from either the Data Provider or Data Recipient regarding a submitted Business Use Case Proposal. The Risk Management Subcommittee shall attempt to mediate the dispute between the Data Provider and Data Recipient. If it appears to the Risk Management Subcommittee that no

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

compromise can be reached between the disputing CHHS Departments, then the CHHS Agency Information Officer and the CHHS General Counsel will elevate the disputed Business Use Case Proposal to the Undersecretary for final decision. The Risk Management Subcommittee shall provide recommendations to the Undersecretary for consideration.

- i. Data. As used in this Agreement, data shall mean any and all personal information, as defined by the California Information Practices Act at Section 1798.3 of the Civil Code, that are transmitted from one CHHS Department to another CHHS Department, including but not limited to, a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means. It excludes departmental personnel records, held as employment records. It may also exclude de-identified data and public documents and data, as defined by the Public Records Act (Cal. Government Code § 6250 et seq.).
- j. Data Protection. Multiple technologies deployed or data protection capabilities including, but not limited to: 1) specific access controls; 2) field by field redaction; 3) upstream and downstream filtering; 4) encryption; and 5) filtering logic to restrict quantity of data provided.
- k. Data Provider. A Data Provider is a CHHS Department or unit or program within a CHHS Department that provides data from specified data source systems to a Data Recipient.
- l. Data Recipient. A Data Recipient is a CHHS Department or unit or program within a CHHS Department and its specific Authorized User groups, which have been approved to access or receive data from a Data Provider.
- m. Data Source Systems or CHHS Source Systems. Data Source Systems are individual data source system(s) that are electronic information storage systems for data elements or information from Data Providers.
- n. Governance Liaison. The Governance Liaison is the Deputy Agency Information Officer who is responsible to facilitate review and decision on disputed Business Use Case Proposals. Data Recipients and Data Providers shall submit disputed Business Use Case Proposals to the Governance Liaison for facilitation through the review and decision process. The Governance Liaison shall refer all disputed Business Use Case Proposals to the CHHS Risk Management Subcommittee for decision. The Governance Liaison may independently refer a disputed Business Use Case Proposal to CHHS Governance Advisory Subcommittees for review and recommendations when appropriate. The Governance Liaison shall collect and submit comments and recommendations on disputed Business Use Case Proposals from CHHS Governance Advisory Subcommittees to the CHHS Risk Management Subcommittee. The Governance Liaison shall track all Business Use Case Proposals and evaluate the tracking log for trends and use the tracking log to improve CHHS business processes.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

- o. Permitted Uses. Access to and use of data provided by way of this Agreement is restricted to Authorized Users. Data shall be maintained as confidential and shall only be used for authorized purposes directly related to the carrying out of Authorized Users' functions and responsibilities consistent with undisputed or approved Business Use Case Proposal(s).
- p. Provisioning. Provisioning refers to Data Recipients providing access privileges to Authorized Users. Provisioning is separate and distinct from the vetting process used to authorize a user to access data.
- q. Required by Law. As used in this Agreement, required by law means a mandate contained in law that compels a CHHS Department to make a use or disclosure of data. Required by law includes, but is not limited to, court orders, statutes, and/or regulations.
- r. Undisputed Business Use Case Proposal. An undisputed Business Use Case Proposal is a Business Use Case Proposal that has not been objected to by a Data Provider. The Data Recipient shall briefly explain how and why the matter is undisputed as part of the Business Use Case Proposal. Undisputed Business Use Case Proposals do not need to go through the formal vetting approval process. A Business Use Case is automatically considered approved if undisputed.
- s. User Group. A unit or program within a Data Recipient authorized to access information from Data Provider data source systems. Access is based upon the undisputed or approval of a Business Use Case Proposal. Access shall be consistent with the undisputed or approved Business Use Case Proposal(s).
- t. "Covered entity," "business associate," "hybrid entity," and "protected health information" shall have the same meaning as defined in 45 C.F.R. § 160.103. "Covered component" shall have the same meaning as "health care component" as defined in 45 C.F.R. § 164.103. "Security incident" shall have the same meaning as defined in 45 C.F.R. § 164.304. "Breach" shall have the same meaning as defined in 45 C.F.R. § 164.402.

## II. DATA EXCHANGE AGREEMENT TERMS AND CONDITIONS

- A. *This section establishes the terms and conditions related to CHHS Department responsibilities regarding the provision of data by Data Providers, and the access to and use of data by Data Recipients, when shared through any CHHS applications or infrastructure, as specified.*

The undersigned CHHS Departments agree to the following terms and conditions:

- 1. CHHS Departments agree to collaborate on Business Use Cases and work together to create Business Use Case Proposals. All undisputed Business Use



## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

Case Proposals, including exchanges that are required by law, shall be provided to the Governance Liaison by the Data Recipient.

2. If a Data Provider objects to a business use case, the objecting Data Provider shall provide an explanation for the objection to a Business Use Case Proposal to the Governance Liaison. The explanation provided shall be considered during the vetting process.
3. Each CHHS Department shall provide, access, and/or use the data only for permitted purposes and only to the extent necessary, consistent with all applicable federal, state, and local laws; rules and regulations; and consistent with the CHHS Department 's undisputed or approved Business Use Case Proposal(s).
4. The CHHS Risk Management Subcommittee and/or the Undersecretary shall have discretion to determine access to data elements contained within CHHS data source system(s) based upon applicable laws, rules, regulations, contracts, and policies. Further, each Data Recipient shall have sole discretion to add additional access restrictions, beyond any imposed by the Risk Management Subcommittee, and based upon applicable laws, rules, regulations, contracts, and business policies.
5. Each CHHS Department is responsible for protecting the confidentiality of data and shall implement administrative, physical, and technical safeguards based upon applicable laws, regulations, policies, or other rules that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic data that it creates, receives, maintains, or transmits.
6. CHHS Departments shall take all reasonable steps to maintain the security of shared data. Further, each CHHS Department is responsible for overseeing the actions of its employees with respect to the provision of, use of, and access to the data that is shared pursuant to this Agreement.
7. CHHS Departments shall also ensure in a written agreement that any agent, contractor, or subcontractor to whom it provides data agrees to implement reasonable and appropriate safeguards to protect and maintain such CHHS data consistent with federal and state laws, including but not limited to, the Information Practices Act and applicable requirements of the State Administration Manual Chapter 5300.
8. Each CHHS Department agrees that its employees will conduct business consistent with their authorization(s) to participate and further agrees to take appropriate action, which may include discipline and restrictions on access, where such authorization has been violated and/or misused.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

9. Each CHHS Department agrees that all sharing of data shall be in accordance with all applicable laws, rules, and regulations.
10. Each CHHS Department is responsible for the maintenance of its own data source system.
11. Each CHHS Department shall only modify its own data.
12. CHHS Departments shall immediately remove an Authorized User's access to CHHS source systems if the Authorized User no longer qualifies as an Authorized User due to improper access, use, and/or disclosure.
13. CHHS Departments shall immediately remove an Authorized User's access to CHHS source systems if such Authorized User's role and responsibilities change and the user is no longer performing the functions of permitted uses consistent with the CHHS Department's Business Use Case Proposal, or the Authorized User is no longer employed by the CHHS Department.
14. Should a CHHS Department stop exchanging data with another CHHS Department based upon statutory, regulatory, or contractual changes, or based on such other CHHS Department's acts in connection with CHHS source systems or this Agreement, the CHHS Department shall immediately notify the Governance Liaison and the Risk Management Subcommittee of the reasons in support of such action or if proposed but not yet taken, a request to take such action.
15. This Agreement eliminates the need for CHHS Department s to enter into "point-to-point" agreements with each other for the same data and purpose(s) associated with CHHS source systems and undisputed or approved Business Use Case Proposals, except where a different agreement is required by the federal government or federal law regarding use and sharing of data obtained by the federal government that is shared with CHHS Departments.
16. CHHS Departments that intend to be Data Providers and/or Data Recipients shall provide a Certification to the Governance Liaison and the Risk Management Subcommittee that represents and affirms in writing they have adequate data protection consistent with federal and state laws and regulations.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

*B. In addition to the terms and conditions above set forth for all CHHS Departments, each Data Provider and Data Recipient additionally agrees to the following specific set of terms and conditions:*

### Data Providers

1. The undersigned Data Providers represent and affirm that they shall authorize access to data by Authorized Users in accordance with all applicable federal, state, and local laws; rules, regulations, and policies; and that such data may be shared pursuant to this Agreement consistent with the original purposes of its collection without consumer consent.
2. Data Providers agree to transmit their data and, to the extent consistent with their governing statutes, regulations, existing contracts, rules and policies, to make such data accessible in whole or in part for use by approved Data Recipients and their Authorized Users for purposes described in undisputed or approved Business Use Case Proposals.
3. When Data Providers use specialized security requirements unique to the data in excess of the baseline described herein, that may be required by federal agencies such as the Social Security Administration, Data Providers shall communicate these additional security measures to Data Recipients. Any additional security requirements shall be set forth within the Business Use Case Proposal as part of the proposal. Data Recipients shall implement the additional security requirements consistent with the Business Use Case Proposal.
4. Data Providers may terminate access to a CHHS source system and/or transmission of data to any Data Recipient if the Data Provider determines that the Data Recipient has violated a material term of this Agreement. A Data Provider terminating access to a CHHS source system and/or transmission of data to a Data Recipient shall immediately notify the Governance Liaison and the Risk Management Subcommittee.
5. Data Providers may exclude certain data and/or records based upon applicable laws, rules, contracts, and/or regulations. However, Data Providers may not exclude data on a disputed but approved Business Use Case Proposal.
6. Data Providers are expected to maintain their own data, and provide data definitions if data will be sourced from them.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

### Data Recipients

1. No Use by Other than Authorized Users. Data Recipients shall restrict access to data and CHHS source systems to Authorized Users and only for authorized purposes, as described in undisputed or approved Business Use Case Proposals.
2. All information accessed from CHHS source systems shall be held confidential to the extent required by law, and shall only be used for authorized purposes directly related to the carrying out the Authorized Users' functions and responsibilities consistent with Data Recipient's undisputed or approved Business Use Case Proposals.
3. Each Data Recipient shall ensure that Authorized Users are trained prior to accessing a CHHS source system, explanation of the guidelines for access and use of data, and security requirements and the proper handling and use of data. Each Data Recipient shall also ensure Authorized Users receive updated training on a periodic basis.
4. Each Data Recipient shall use any necessary administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of data accessed from CHHS source systems.
5. Each Data Recipient shall immediately report to a Data Provider and the Governance Liaison any access, use, or disclosure of data not permitted or required by this Agreement, or an undisputed or approved Business Use Case Proposal(s), or as required by law.
6. Each Data Recipient shall immediately report to a Data Provider and Governance Liaison any information security incident involving loss, theft, damage, misuse of information assets, or improper dissemination of data of which it becomes aware. Data Recipients shall also immediately notify Data Providers of any use or disclosure of data inconsistent with this Agreement or the undisputed or approved Business Use Case Proposal(s) of which it becomes aware.
7. Each Data Recipient shall not further disclose data unless required by law or as authorized in the Data Recipient's undisputed or approved Business Use Case Proposals.
8. Data Recipients shall ensure in written contract that contractors, consultants, and subcontractors that create, receive, store, or transmit data on behalf of the Data Recipient agree to the same restrictions, requirements, conditions that apply to the Data Recipient with respect to data.
9. At termination of the business use case, the Data Recipient shall return or destroy the data provided consistent with the undisputed or approved Business Use Case Proposal unless an alternative is stated in the undisputed or approved Business Use Case Proposal. If the data cannot be returned or destroyed, the Data Recipient shall continue to safeguard the information and limit further uses or disclosure to those

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

purposes that make return or destruction infeasible. If circumstances change and, as a result, the data cannot be returned or destroyed consistent with the approved Business Use Case Proposal(s), the Data Recipient must inform the Data Provider, Governance Liaison, and Risk Management Subcommittee within 10 days of an alternative method with a description of data protections.

10. Due to the differences in collection practices that are specific to individual departmental needs, requests for data about a particular consumer may not always yield data with the identification demographics provided. It is possible that demographics and identifying information collected by one Department differs from demographics and identifying information collected by another. Departments shall work together on identifying information and demographics when it is likely a consumer receives services from more than one Department.
11. Each Data Recipient shall ensure that Authorized Users understand that improper use or disclosure is in violation of such CHHS Department's policies and will result in appropriate action, including potential disciplinary action, and may also subject such employee to civil or criminal penalties.

### **III. MEMORANDUM OF UNDERSTANDING FOR HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES**

*This portion of the Agreement only applies to CHHS Departments that meet the definition of covered entity or business associate as defined at 45 C.F.R. § 160.103 or that meet the definition of hybrid entity as defined at 45 C.F.R. § 164.103.*

The undersigned covered entity and business associate CHHS Departments agree to the following:

1. Each Department is responsible for protecting the confidentiality of data and shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of protected health information that it creates, receives, maintains, or transmits consistent with federal laws and standards and the State Administration Manual Chapter 5300.
2. Data Providers and/or Data Recipients shall ensure in a written agreement that any agent, contractor, or subcontractor to whom it provides protected health information, agrees to implement reasonable and appropriate safeguards to protect data consistent with federal and state laws, including but not limited to, the Information Practices Act and the Health Insurance Portability and Accountability Act. This Agreement shall satisfy this requirement between CHHS Departments.
3. Data Providers may terminate access to a CHHS source system and/or transmission of data to any Data Recipient if the Data Provider determines that the Data Recipient has violated a material term of this Agreement. A Data Provider terminating access to a CHHS source system and/or transmission of data to a Data Recipient shall immediately notify the Governance Liaison and the Risk Management Subcommittee.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

4. Each Data Recipient shall use any necessary administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of data accessed from CHHS source systems. Business associate Departments that are Data Recipients shall comply with Subpart C of 45 C.F.R. Part 164 with respect to protected health information to prevent use and disclosure not permitted or required by this Agreement, undisputed or approved Business Use Case Proposal(s), or as required by law.
5. Each business associate that is a Data Recipient shall immediately report in writing to a Data Provider and the Governance Liaison any security incident and breach of which it becomes aware. Business associate Departments that are Data Recipients shall also immediately notify Data Providers of any use or disclosure of data inconsistent with this Agreement or the undisputed or approved Business Use Case Proposal(s) of which it becomes aware.
6. A Data Recipient shall not further disclose data unless required by law or consistent with the Data Recipient's undisputed or approved Business Use Case Proposals.
7. Business associate department s that are Data Recipients shall make available protected health information to patients when requested in accordance with 45 C.F.R. § 164.524. Business associate Departments that are Data Recipients shall make available protected health information for amendment and incorporate amendment in accordance with 45 C.F.R. § 164.526. Business associate Departments that are Data Recipients shall also make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528.
8. With respect to protected health information, business associate Departments that are Data Recipients agree to use and disclose data only as permitted or required by the undisputed or approved Business Use Case Proposal(s) or as required by law.
9. When an undisputed or approved Business Use Case Proposal or other obligation requires a business associate that is a Data Recipient to carry out a covered entity Data Provider's obligation under Subpart E of 45 C.F.R. Part 164, the business associate that is a Data Recipient shall comply with the requirements of Subpart E that apply to the covered entity Data provider in performance of its obligations to the covered entity Data Provider.
10. A business associate that is a Data Recipient shall make its practices, personnel, books, records, and policies regarding the use and disclosure of protected health information available to the Secretary of the federal Health and Human Services when requested to determine the compliance of the covered entity Data Provider.



11. Business associate Departments that are Data Recipients shall ensure in written contract that contractors, consultants, and subcontractors that create, receive, store, or transmit protected health information on behalf of the business associate that is a Data Recipient agree to the same restrictions, requirements, conditions that apply to the business associate that is a Data Recipient with respect to protected health information.
12. At termination of the business use case as approved in the Business Use Case Proposal the Data Recipient shall return or destroy the data provided consistent with the undisputed or approved Business Use Case Proposal. If the data cannot be returned or destroyed, the Data Recipient shall continue to safeguard the information and limit further uses or disclosure to those purposes that make return or destruction infeasible. If circumstances change and, as a result, the data cannot be returned or destroyed consistent with the undisputed or approved Business Use Case Proposal(s), the Data Recipient must inform the Data Provider and Governance Liaison within 10 days of an alternative method with description of data protections.

#### IV. CONTROLLING LAWS, RULES, AND REGULATIONS

**Change Required to Comply with Applicable Law.** Notwithstanding any prior approvals regarding the sharing of information, if a change is required regarding authorized use(s) to comply with statutory and/or regulatory changes, CHHS Departments shall notify the Governance Liaison and the Risk Management Subcommittee to implement such change in compliance with all applicable laws, rules and regulations. All impacted CHHS Departments shall be notified by the Governance Liaison and the Risk Management Subcommittee in the event of a change required to comply with applicable law. Business Use Case Proposals are required to be updated in the event of a change in law, when necessary to comply with applicable law.

#### V. IMPROPER USE AND DISCLOSURE

1. Access to CHHS data source systems is restricted to Authorized Users.
2. All data accessed from a CHHS source system shall be held confidential to the extent required by law, and shall be used by Authorized Users solely for carrying out their functions and responsibilities as Authorized Users directly related to and consistent with Data Recipient's undisputed or approved Business Use Case Proposal(s).
3. Improper use or disclosure is in violation of CHHS Policy and applicable laws, rules, and regulations.

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

4. Any individual who has engaged in improper use or disclosure of CHHS source system data will be subject to his or her Department's disciplinary process.
5. Any individual who has engaged in improper use or disclosure of CHHS source system data may be subject to civil and/or criminal penalties.
6. CHHS Departments shall immediately remove an Authorized User's access to a CHHS source system if the Authorized User has engaged in improper use and/or disclosure. CHHS Departments shall have policies and procedures addressing the protocol for investigating and removing access when an Authorized User is suspected of engaging in improper use and/or disclosure. CHHS Departments shall follow their internal policies and procedures when an Authorized User is suspected of engaging in improper use and/or disclosure.
7. Required Notice to Data Providers: Should data obtained from a CHHS source system be improperly released (for example, misplaced or stolen, or disclosed in an unauthorized manner) or where the Data Recipient discovers evidence of willful or intentional misuse of data, the Data Recipient shall inform the Governance Liaison, the Risk Management Subcommittee, and the Data Provider whose data has been improperly released or misused immediately upon discovery by the Data Recipient.

### VI. DISCLAIMERS

Reliance on a Data Source System: Nothing in this Agreement shall be deemed to impose responsibility or liability on a CHHS Department related to the accuracy, content, or completeness of any data provided pursuant to this Agreement. The CHHS Departments acknowledge that other CHHS Departments may be added or terminated at any time; therefore, CHHS Departments may not rely upon the continued availability of a particular CHHS Department's data.

### VII. SECURITY

Multiple technologies shall be deployed with data protection capabilities on CHHS source systems, including: 1) role based access controls; 2) field by field redaction where applicable; 3) upstream and downstream firewall filtering; 4) encryption of data in motion; 5) encryption of data at rest on end points; 6) filtering logic to restrict quantity of data provided ; and 7) auditing. Each CHHS Department certifies it has in place a system that provides policy-based authentication and authorization of users. Access is obtained only by individuals whose credentials are verified upon Log-In and have been approved by their CHHS Department. Each source system filters data based upon Authorized Users assigned role and agency. Activities will be recorded in security audit logs. All use will be subject to compliance with CHHS and CHHS Departmental policies and procedures for data access, use, and disclosure.

#### **VIII. SEVERABILITY**

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid, by any court that invalidity shall not affect the other provisions of this Agreement and the invalid provision(s) shall be considered modified to conform to the existing law.

#### **IX. ADDITIONAL CHHS DEPARTMENTS**

The undersigned CHHS Departments acknowledge that additional CHHS Departments (Data Providers and/or Data Recipients) may be added to this Agreement. All current CHHS Departments agree that, prior to admission of a new CHHS Department, the new CHHS Department must agree to be bound by the terms of this Agreement. An additional CHHS Department, if not a current signatory, shall stipulate to all the terms of this Agreement. The CHHS Department s agree that upon such stipulation by a duly authorized representative of such additional CHHS Department, such additional CHHS Department shall be deemed to be a signatory to this Agreement and will be bound by all the terms of this Agreement.

#### **X. EFFECTIVE DATE**

This Agreement shall remain in full force and effect immediately from the date of execution by a duly authorized representative of a CHHS Department.

#### **XI. MODIFICATION/TERMINATION**

This Agreement may only be modified or terminated in writing by mutual consent of all signing CHHS Departments.

#### **XII. ENTIRE AGREEMENT**

All undisputed and approved Business Use Case Proposals are incorporated by reference herein. No verbal agreement shall, in any way, vary or alter any provision of this Agreement. Aside from undisputed or approved Business Use Case Proposals, this written Agreement:

- Contains all the terms and conditions agreed upon by the parties hereto.
- Constitutes the full and complete agreement between the CHHS Departments.

No other written agreement shall, in any way, vary or alter any provision of this Agreement unless modified in writing by mutual consent of all CHHS Departments or as required by statutory or regulatory changes.

### XIII. SIGNATURES

**The undersigned hereby accept and agree to be bound by all of the provisions and terms and conditions set forth in this Intra-Agency Data Exchange Agreement.**

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Secretary, California Health and Human Services Agency

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Undersecretary, California Health and Human Services Agency

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Agency Information Office, California Health and Human Services Agency

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Aging

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Child Support Services

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Community Services and Development

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Developmental Services

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Health Care Services

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Managed Health Care

*Original signed by*

\_\_\_\_\_, Date \_\_\_\_\_  
Director, Department of Public Health

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Department of Rehabilitation

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Department of Social Services

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Department of State Hospitals

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Emergency Medical Services Authority

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Assistant Director, Office of Health Information Integrity

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Chief, Office of Law Enforcement Support

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Office of the Patient Advocate

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Office of Statewide Health Planning and Development

*Original signed by*

\_\_\_\_\_. Date \_\_\_\_\_

Director, Office of Systems Integration

## **Montgomery County, Maryland—Notice of Privacy Practices**

---

The Department of Health and Human Services (DHHS) of Montgomery County, Maryland, is a large, multi-service agency that provides health, mental health, substance abuse, child welfare, income support, and other social services. DHHS provides its Notice of Privacy Practices to all individuals who apply for services to inform them about DHHS' legal obligation to protect individuals' information, how their information will be shared, their rights related to their information, and who to contact to ask questions, make a request, or file a complaint.



## NOTICE OF PRIVACY PRACTICES

**THIS NOTICE DESCRIBES HOW YOUR HEALTH AND OTHER PERSONAL INFORMATION MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS CAREFULLY.**

### Our Services and Information We Collect

The Montgomery County Department of Health and Human Services (DHHS) is a large, multi-service agency that provides health, mental health, substance abuse, child welfare, income support and other social services. To provide you with services, DHHS staff will ask you for personal information that they will keep in your records. This information may include:

- Information that identifies you, such as your name, address, telephone number, date of birth and social security number.
- Financial information, which includes information about your income, your bank accounts or other assets, and any insurance coverage that you have.
- Protected health information, which includes any information that tells us about your past, present or future health or mental health treatment.
- Information about benefits or services that you are receiving or have received.

### Our Responsibilities

Federal and State laws protect the privacy of your health and other personal information and we will follow all of those laws. We will take reasonable steps to keep your information safe, and will use (share within DHHS) and disclose (share with persons outside of DHHS) your information only as necessary to do our jobs and as permitted or required by law. We are required to let you know if a breach occurs that may have compromised the privacy or security of your health information.

If we have a need to use or disclose your information for any reason other than those listed below, we will ask you for your written permission. You have a right to cancel any written permissions you have given to us. If you cancel your permission, the cancellation will not apply to uses and disclosures that we have already made based on your permission.

We are required by law to provide you with this notice and to follow it. We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on the DHHS website at [www.montgomerycountymd.gov](http://www.montgomerycountymd.gov).

### How We May Use and Disclose Your Information

- **For Treatment and Services:**  
DHHS staff who work with you may use your health and other personal information as necessary to provide you with coordinated treatment and services. DHHS has implemented an integrated case management system and an electronic health record to store your health and other personal information. We may gather information about you from other health care providers you have



seen, healthcare facilities that have run tests on you, your health insurance plan and, sometimes, even family members or close friends that help take care of you. Some or all of your medical information may be created and/or stored in an electronic format.

Examples:

- If you are receiving health care from one of our clinics and want to apply for other services such as housing assistance or income supports, your case worker can help you access those services by making referrals and sharing eligibility information.
- If you are receiving more than one DHHS service, your case workers may communicate with one another to develop a coordinated service plan with you when appropriate.

When permissible for valid purposes (e.g., providing treatment or billing for services) your health care providers may access your medical information electronically. Other healthcare providers outside DHHS caring for you may also receive access to your electronic records.

We will share your information with persons outside of our DHHS agency for treatment or services only with your written permission or as allowed by federal or State law. For example, federal and State laws permit our DHHS staff that provide you with health care to share your health information with outside health care providers who are also treating you.

### **If you receive behavioral health services from us:**

- Your mental health records may be shared to provide you with treatment or services without your authorization, but we will only share information that is relevant to your treatment or service plan.
- We maintain one electronic health record for your health and behavioral health information so that our health care providers can make informed treatment decisions and coordinate your health care.
- Most sharing of psychotherapy notes will be done only with your written authorization. Psychotherapy notes are defined by law as notes created by a mental health professional that are kept separate from your health record. In general, our staff include all of their notes in your health record and do not maintain separate psychotherapy notes.
- We will not share your alcohol or substance abuse program records unless:
  - You have given us your written permission;
  - The disclosure is allowed by court order;
  - The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit or program evaluation;
  - We are sharing with someone who is providing services to you or our program, and we have an agreement in place to protect the information. *We have these agreements in place to allow your substance abuse program records to be shared with your DHHS health and behavioral health care providers.*
- We will not share your information from our Abused Persons, Victim's Assistance and Sexual Assault Programs without your written permission except as permitted or required by law. These programs are restricted within our electronic systems.

Some of our programs maintain records that are considered "education records" under the Family Education Rights and Privacy Act of 1974 ("FERPA"). We will not share information about you from these records with other service providers without your written permission unless it is necessary to address an emergency.

DHHS has chosen to participate in the Chesapeake Regional Information System for our Patients, Inc. (CRISP), a regional health information exchange (HIE). As permitted by law, your health

information may be shared with this exchange in order to provide faster access, better coordination of care and assist providers and public health officials in making more informed decisions. You may “opt out” and prevent searching of your health information available through CRISP by calling 1-877-952-7477 or completing and submitting an Opt Out form to CRISP by mail, fax or through their website at [www.crisphealth.org](http://www.crisphealth.org). If you opt out of participation in CRISP, your health care providers will still be able to select the HIE as a way to receive your lab results, radiology reports, and other data sent directly to them that they may have previously received by fax, mail or other electronic communications. Legally mandated public health reporting, such as the reporting of infectious diseases to public health officials, will also occur through the HIE after you decide to opt out.

**Health Information.** We may use or disclose your health information to provide information to you about treatment alternatives, other services or other health related benefits and services that may be of benefit to you.

**DHHS Directory.** Unless you object, we may use your health information, such as your name and general demographic information for our directory. The information contained in our directory will not be disclosed to individuals outside of our health and human services environment with your authorization.

- **For payment:** We may use or disclose health and other personal information about you as necessary to obtain payment for health and mental health services received. For example, we may use your information to bill Medicaid or Medicare for treatment you received.
- **For Health Care/Business Operations:** We may use or disclose your health and other personal information to manage our programs or activities. For example, DHHS staff or outside auditors may look at your case record to review the quality of services you received through our department.
- **For Appointments or Notifications:** We may need to contact you or your representative, to schedule or remind you of an appointment, to ask you to complete paperwork, to inform you about other related benefits or services that you may be interested in, or to reach you in an emergency.
- **To our Business Associates:** We have agreements with persons outside of DHHS that perform services on our behalf, or provide us with administrative and support services, such as financial or legal services, data analysis, and accreditation and quality assurance reviews. These persons are called business associates. We may disclose your information to business associates so that they can perform these services for us. However, we require our business associates to keep your information safeguarded.
- **To your Family, Friends and Others Involved in Your Care:** We may disclose your health information to your family or others who are involved in your medical care. For example, we may discuss your medical condition with your adult daughter or son who is arranging for your care at home. If you do not want us to share this information with your family, you can ask that we not do so. We will not share information about your mental health or substance abuse history or care with your family unless you give us written permission.
- **For Government Programs:** We may disclose health and other personal information about you to determine if you are eligible for other government benefits or programs such as Social Security benefits.

- **For Public Health Activities:** We may use or disclose health information about you for public health activities. For example, if you have been exposed to a communicable disease (such as a sexually transmitted disease), we may report it to the State and take other actions to prevent the spread of this disease.
- **For Health Oversight Activities:** We may disclose your information as required by law to other agencies who oversee our programs for oversight activities such as audits, inspections, investigations, and licensure.
- **For Abuse and Neglect Reports and Investigations:** We are required by law to report any cases of suspected abuse or neglect of children or vulnerable adults, including adults abused as children. Health and mental health providers are required by law to share information with adult and child protective services if the health/mental health care provider believes the information will contribute to the protective service investigation, assessment of risk, or service/safety plan.
- **To Avoid Harm:** DHHS may disclose health and other personal information about you to law enforcement under certain conditions. For example, if you harm a member of our staff or another client, if you damage our property or if our professional staff believes that you are likely to cause serious harm to others or yourself, we will contact law enforcement. DHHS may also disclose your health and other personal information in case of a threat to the public, such as a terrorist attack or emergency disaster.
- **To Coroners, Funeral Directors, Medical Examiners and for Organ Donation:** DHHS may disclose health information relating to death to coroners, medical examiners and funeral directors and also to authorized organizations relating to organ, eye or tissue donations or transplants.
- **For Research Purposes:** We may use or disclose your health information for medical research purposes under certain circumstances. In some cases, your written permission will be needed. Research studies and reports will not identify people by name.
- **For Court proceedings:** We may be required by law or court order to provide information about you to the court. We may also share health information about you for workers' compensation claims.
- **As Required by Law:** If a law or regulation requires that we disclose your health or other personal information, we must do so.
- **Fundraising:** We generally do not engage in fundraising with our clients, but if we contact you for fundraising efforts, you can tell us not to contact you again.
- **Health Information Availability After Death.** DHHS may use or disclose your health information without your authorization fifty (50) years after your death. You have the right to restrict those disclosures.

### **Your Rights Regarding your Information**

#### **You have the right to:**

- Obtain a copy of this notice. This notice is available in alternative format upon request.
- Ask us to contact you at a different location or to contact you by a different method than we routinely use. For example, you may ask that we contact you by phone or mail at work instead of at home.

- See, review and receive a copy of information we maintain about you. *You must make this request in writing* and you may be charged a fee to pay for the cost of copying your record. There are certain situations when we may not give you the right to review or obtain a copy of your records. If this happens, we will explain why. If we maintain your health information in an electronic record, you can also ask for your information in an electronic format.
- Ask us to correct information about you that you think is incorrect or incomplete. *You must do this in writing*. In some situations, we are not required to make the change. If we do not agree to make the change, we will explain why.
- Ask for a list (accounting) of the times we have disclosed your health information for six years prior to the date you ask. This listing will not include disclosures made for treatment, payment or health care operations purposes, or disclosures you have permitted us to make. *You must make this request in writing*.
- Request that we not share health information with a family member or others involved in your care.
- Request that we not share your information for a treatment/service, payment or health care operations purpose. *These requests must be made in writing*. We are not required to agree to these requests, but if we do, we must comply with the agreement, unless we need to disclose the information for your emergency treatment. If we cannot agree to your request, we will explain why.
- If you pay for a service or health care item out of pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will agree to comply with your request unless a law requires us to share that information.
- Require that we obtain your written permission if we want to sell your information or share your information for marketing purposes.
- Receive a notification from us if there is ever a breach of your information.
- File a complaint or report a problem if you feel we have violated your rights. We will not take any action against you for filing a complaint. To file a complaint or report a problem contact our Privacy Officer at the following address:

Privacy Officer  
Montgomery County Department of Health and Human Services  
401 Hungerford Drive  
Rockville, MD 20850  
240-777-1295 (Voice)  
[PrivacyMatters@montgomerycountymd.gov](mailto:PrivacyMatters@montgomerycountymd.gov)

If your complaint relates to your *health* information, you may also contact the U.S. Department of Health and Human Services, Office for Civil Rights by calling 1-877- 696- 6775.

### **How to Make a Request**

If you have questions about our privacy practices or want to make a request for any of the above, contact the staff person who is working with you, or our Privacy Official at the address listed above. We ask that you use the *DHHS Client Request Form* for requests that must be made in writing. You can obtain the form from any DHHS office or by contacting our Privacy Officer.

*Effective Date: This notice is effective on June 7, 2019.*

## **State of Indiana – Memorandum of Understanding**

---

This is a Memorandum of Understanding between the Indiana Department of Health (“ISDH”) and the Indiana Family and Social Services Administration (“FSSA”) for the purpose of sharing and exchanging data as permitted or required by federal and state laws and regulations. The MOU establishes the mutual understanding of the roles and responsibilities of the parties with respect to all current and future electronic data exchanges between ISDH and FSSA.

**Memorandum of Understanding  
Between  
The Indiana Department of Health  
And  
Indiana Family and Social Services Administration  
Number xxx-x-xx-xx-xx-xxxx**

This Memorandum of Understanding (“MOU”) is entered into by and between the Indiana Department of Health (“ISDH”) and the Indiana Family and Social Services Administration (“FSSA”), including all of its divisions. In consideration of the mutual understandings and covenants set forth herein, the parties agree as follows:

**I. INTRODUCTION AND PURPOSE**

- a. ISDH and FSSA, through its various divisions, routinely exchange data in electronic format in support of programs undertaken by each agency in which shared information is necessary for the successful execution of such programs. Such data exchanges are either permitted or required by applicable federal and/or state laws and regulations and support a defined business need with respect to the associated programs.
- b. In order to minimize the number of agreements entered into by and between ISDH and FSSA regarding such data exchanges, and in order to assure consistency of the terms and conditions that apply to all such data exchanges, the parties wish to enter into a single agreement (this MOU) that includes a definition of each such data exchange attached hereto as appendices.
- c. The purpose of this MOU is to establish a mutual understanding of the roles and responsibilities of the parties with respect to all current and future electronic data exchanges between ISDH and FSSA as set forth in the appendices to this MOU.
- d. Upon execution this MOU contains Appendices X through X. These appendices do not contain separate signatures. Additional or amended appendices will be added in accordance with Section III Amendment.

**II. TERM AND TERMINATION**

- a. This MOU shall be effective [date] and shall terminate on [date].
- b. This MOU may be renewed for successive two (2) year terms upon mutual written agreement between the parties. Any renewal of this MOU will include all appendices attached hereto at the time of the renewal unless otherwise stipulated at the time of the renewal.
- c. This MOU may be terminated with or without cause by either party upon thirty (30) days written notice to the other party.
- d. When the Director of the State Budget Agency makes a written determination that funds are not appropriated or otherwise available to support continuation of performance of this MOU, the MOU shall be cancelled. A determination by the Director of the State

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

Budget Agency that funds are not appropriated or otherwise available to support continuation of performance shall be final and conclusive.

### III. AMENDMENT

- a. This MOU may be amended at any time by mutual written agreement of the parties; provided however:
  - i. With respect to an appendix only, an appendix may be added, removed, or modified by mutual written agreement of ISDH and the FSSA Division of Healthcare Strategies and Technology.
  - ii. Appendices do not need to be amended to reflect minor changes in the data fields that do not otherwise materially affect the data exchange or legal authorities cited therein.

### IV. FUNDING

This MOU is hereby established as a no-cost agreement between the parties. Any data sharing exchanges between ISDH and FSSA that involve the exchange of funds will be addressed in separate MOUs.

### V. AUTHORITY

This MOU is executed under the authority of IC 12-8-1.5-6.

### VI. PROVISIONS

- a. ISDH and FSSA agree to undertake specific electronic data exchanges as defined in each of the appendices attached hereto.
- b. The data to be exchanged, including but not limited to, sending party, receiving party, meta data, data source, frequency of the exchange, data selection criteria, method and means of the exchange (e.g., secure file transfer), and additional considerations will be defined in the appendix for each exchange.
- c. Each appendix for each data exchange will cite the business purpose (including program) for the exchange and the legal authorities under which the data exchange is permitted or required.
- d. The term for each data exchange will be identified in the applicable appendix. By way of example only, some exchanges may be only required for a short period of time; others may continue for as long as this MOU continues in force, including renewals.



## VII. CONFIDENTIALITY AND SECURITY OF THE DATA

- a. ISDH and FSSA agree that each is required to secure and protect the confidentiality, integrity, and availability of confidential data in its safekeeping, including but not limited to Protected Health Information<sup>1</sup> and Personal Information<sup>2</sup>, in compliance with applicable federal and state laws and regulations. These laws and regulations include, but are not limited to, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), including regulations and subsequent amendments thereto, Indiana Code 4-1-10, Indiana Code 4-1-6, 42 C.F.R. Subpart F, 7 C.F.R. § 205.50, Indiana Code 12-15-27, Indiana Code 12-14-1, and the Patient Protection and Affordable Care Act (Public Law 111-148).
- b. Data provided to one party (the “receiving party”) by the other party (the “sending party”) under this MOU (the “Data”) will be kept secure and confidential (collectively, “safeguarded”) by the receiving party (inclusive of any third parties performing services on behalf of the receiving party and to which access and use of such Data is authorized by the receiving party) in accordance with applicable state and federal laws and regulations and not used or disclosed outside of the purpose for which the Data was provided under this MOU, excepted as otherwise may be required by law.
- c. Should a breach of confidentiality occur, meaning that the Data in the safekeeping of the receiving party has been used or disclosed in a manner not permitted by this MOU or by applicable federal and state laws and regulations (collectively, a “breach”), then:
  - i. The receiving party will undertake appropriate mitigating actions as prescribed by applicable federal and state laws and regulations, including providing notice to the victims of the breach and/or other notices to state and/or federal authorities where required.
  - ii. The receiving party will provide prompt notice of the breach to the sending party in the manner described below:
    - (1) When ISDH is the receiving party:
      - (a) Once a breach has been confirmed by the ISDH Security Manager, the ISDH Security Manager will provide an initial awareness notice to the FSSA Privacy and Security Officer within twenty-four (24) hours of such confirmation; such notice may be made by phone (877-690-0010 or 317-232-4732) or by email ([fssa.PrivacyOffice@fssa.in.gov](mailto:fssa.PrivacyOffice@fssa.in.gov));
      - (b) Subsequently, the ISDH Security Manager (or designee) will periodically update the FSSA Privacy and Security Officer (by email at

---

<sup>1</sup> As defined in 45 C.F.R. § 160.103

<sup>2</sup> Reference IC 4-1-6-1 and IC 4-1-11-3 for examples of Personal Information; also commonly referred to as Personally Identifiable Information.

[fssa.PrivacyOffice@fssa.in.gov](mailto:fssa.PrivacyOffice@fssa.in.gov)) regarding the status of the breach including mitigating actions taken or will be undertaken by ISDH; the timing of such periodic updates will at the discretion of the ISDH Security Manager but made such that the FSSA Privacy and Security Officer is kept reasonably apprised of the status; and

- (c) Upon conclusion of the breach event the ISDH Security Manager will provide the FSSA Privacy and Security Officer with a copy of ISDH's internal breach report or similar report summarizing the breach details and the actions taken.

(2) When FSSA is the receiving party:

Reporting of Security Incident to ISDH. FSSA, in collaboration with FSSA Privacy Office shall report to ISDH any security incident of which the FSSA becomes aware. Successful breaches of security shall be reported by FSSA Privacy Office to the ISDH Security Manager by calling (317) 233-4945 within two (2) hours of becoming aware of the breach **and** in electronic form to [PrivacyandSecurityOfficers@ISDH.in.gov](mailto:PrivacyandSecurityOfficers@ISDH.in.gov) within twenty-four (24) hours of becoming aware of the breach. If the FSSA Privacy Office is unable to reach the ISDH Security Manager at the above phone number, then the FSSA Privacy Office will report successful breaches of security to the Chief Information Officer by calling (317) 233- 7673 within the same timeframes indicated above. In the event a successful breach is discovered outside of normal business hours, leaving a voice message at the above listed numbers is sufficient verbal notification; however, FSSA in collaboration with the FSSA Privacy Office shall still comply with the electronic reporting requirement stated above.

The following format should be used when reporting the breach electronically:

•**Name of Agency**

Incident # (number assigned by reporting entity)

•**Type of Incident –**

Date and Time of Report (Date and time incident was initially reported)

Date and Time of Incident (Date and time incident occurred)

Time potential breach was identified

•**Name and Title of Person Reporting Incident**

Contact Information (of person reporting incident)

•**Summary of Incident** (Include pertinent information regarding the potential security breach)

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

- **Description of Personally Identifiable Information Involved** (Include number of participants records involved)
- **Action Taken**  
Name of Person(s) Conducting Preliminary Investigation Contact  
  
Information (of individual responsible for Issue Analysis) Date  
  
Investigation started  
  
Action(s) Taken (include dates, times, and names of agencies notified of the Incident)
- **Conclusion**  
Measures taken to address issue, and prevent any reoccurrences

- d. All electronic data exchanges between FSSA and ISDH will be secured through encryption technologies that meet or exceed the standards under Federal Information Processing Standards (FIPS) 140-2, Level 1, for data in motion.

### VIII. NOTICE TO THE PARTIES

- a. Where written notice is required under this MOU, such written notice shall be provided to the FSSA Secretary and the Contracts Section of ISDH.
- b. With respect to the performance of an electronic data exchange as defined in an appendix to this MOU, communication shall be between the agency program contacts listed in the applicable appendix.
- c. Each agency will notify the other when there is a change in the program contact listed in an appendix to help facilitate communication.

---

**THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK.**

Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

**In Witness Whereof**, ISDH and FSSA through their duly authorized representatives, enter into this MOU. The parties, having read and understood the foregoing terms of this MOU do, by their respective signatures dated below, hereby agree to the terms thereof.

**Indiana State Department of Health**

_____	_____
Deputy Chief of Staff Chief Financial Officer	Chief of Staff
_____	_____
Date	Date
_____	
Chief Information Officer	
_____	
Date	

**Family and Social Services Administration**

_____	_____
Secretary Family and Social Services Administration	Director Division of Healthcare Strategies and Technology
_____	_____
Date	Date

**State Budget Agency**

_____
OMB Director
_____
Date

## **State of Washington – Forms for Requests from a Data Warehouse**

---

The Washington State Education Research and Data Center employs three forms for requests of its student data. The forms are intended to protect the data from inadvertent disclosure. One form is an Aggregate Data Request Form used to request cross-sector aggregate data with no direct identifiers. A second form is an Individual Data Request Form used to request unredacted aggregate data or individual-level data for 1) an audit or evaluation of an education program with cross-sector data or 2) a study that meets the conditions of the Federal Educational Rights and Privacy Act (FERPA). The third form is an Individual-Level Data Tables (an Excel workbook not shown below) to outline the specific variables requested, including how to define them and to identify the education sector (i.e., early learning, child care subsidy, K-12, etc.) from which the variables come.



For Admin Only  
Request #

## Aggregate Data Request Form

**Instructions:** Use this form to request cross-sector aggregate data with no direct identifiers.  
Still have questions? [Email the ERDC](#) before you submit the form.

### Requester Contact Information

Date Submitted:

Requester's Name:  Requester's Title:

Requester's Organization:  Department:

Email address:  Phone:

Principal Investigator's (PI) Name:  PI Title:

PI's Organization:  Department:

Email address:  Phone:

### Project Information

- Project Title:
- What type of request are you submitting?
  - ☐ New data request
  - ☐ Request for additional data or a "refresh" of data under prior request with ERDC
 

Prior request number (R#):
- What type of project will this data request support? Check the box below.
  - ☐ Mandated government or legislative report
  - ☐ Grant-funded research
  - ☐ Thesis or Dissertation project
  - ☐ Report by a state or local government agency
  - ☐ Other project type (*Explain below.*)

Updated 2/8/2021

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

4. Briefly describe the purpose, scope, and objectives of your project. If this is a follow-up or update of a previous study, please include a link to or copy of the original work. (1,500 characters max)

5. List the question(s) that you hope to answer. Examples: 1) What is the direct postsecondary enrollment rate for students who participated in Running Start [RS] and College in the High School [CIHS], compared to students who did not participate, disaggregated by race/ethnicity? 2) How many WA high school graduates from the 2015 school year enrolled in WA two-year public institutions on a full-time basis?

**Requested Data**

- Please only ask for the minimum data that you need to answer your question(s).
- If you know what your data should look like, send an example table with your form.

6. For whom / what population are you seeking aggregate data? For what time period(s)?  
Examples: 1) All WA students with required graduation year of 2017 who graduated from high school. 2) All WA high school graduates enrolled in WA two-year public institutions between 2016-17 and 2018-19 school years.



## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

7. What information about this population are you seeking? For what time period(s) and comparison groups? What calculations do you want reflected in the final data? *Examples: 1) Postsecondary enrollment rate in fall after high school graduation, for all years of postsecondary enrollment that data is available. 2) Count by year of 2015 WA high school graduates who were enrolled full-time in a WA two-year public institution between 2016 and 2019.*

8. What subgroups (if any) do you need the aggregate data divided into? *Examples: Race/ethnicity, RS participants vs. non-participants, CIHS participants vs. non-participants.*

**Note:** Aggregate data must meet the [Federal Educational Rights and Privacy Act's \(FERPA\)](#) cell size and use restrictions, which affect if/how the ERDC fulfills data requests.

### Timeline

9. What's your ideal date to receive the requested data?

**Note:** ERDC follows a rigorous process for reviewing data requests, as outlined on our [Data Approval Process webpage](#). The time it takes to review and fulfill a request depends on the complexity of the data.

### Requester's Signature

Requester #1's Signature

Title

Date

Requester #2's Signature

Title

Date

Email your **Aggregate Data Request Form** (and example table, if you have one) to the [ERDC Inbox](#).

Thank you for your submission! ERDC will connect with you after reviewing your request.



For Admin Only  
Request #

## Individual Data Request Form

**Instructions:** Use this form to request unredacted aggregate data or individual-level data for 1) an audit/evaluation of an education program with cross-sector data or 2) a study that meets the conditions of the [Federal Educational Rights and Privacy Act \(FERPA\)](#). Still have questions? [Email the ERDC](#) before you submit the form.

### Requester Contact Information

Date Submitted:	<input type="text"/>		
Requester's Name:	<input type="text"/>	Requester's Title:	<input type="text"/>
Requester's Organization:	<input type="text"/>	Department:	<input type="text"/>
Email address:	<input type="text"/>	Phone:	<input type="text"/>
Principal Investigator's (PI) Name:	<input type="text"/>	PI Title:	<input type="text"/>
PI's Organization:	<input type="text"/>	Department:	<input type="text"/>
Email address:	<input type="text"/>	Phone:	<input type="text"/>

### Project Information

- Project Title:
- What type of request are you submitting? Check the box below.
 

☐ New data request  
☐ Request for additional data or a "refresh" of data under prior request with ERDC  

Prior request number (R#):   
 Data-use agreement number (K#):
- What type of project will be supported by this data request? Check the box below.
 

☐ Mandated government or legislative report  
☐ Thesis or Dissertation project  
☐ Other project type (Explain below.)

☐ Grant-funded research  
☐ Report by a state or local government agency

Updated 2/12/2021

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

4. Does your project intend to produce **generalizable knowledge** (research), as defined by the [Washington State Institutional Review Board \(WSIRB\)](#)? ☐ Yes ☐ No
5. Have you received outside funding to conduct this study? ☐ Yes (*Explain below.*) ☐ No
- 
6. Describe the education program(s) that are part of your analysis, including the program name and purpose.
- 
7. Describe the purpose and scope of your project. Explain your project objectives and how you plan to evaluate the program(s).
- 
8. List the key research questions that your project will address.
-

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

9. Describe the project's study population(s), including any comparison groups or cohorts, as well as time elements. (Examples: All special education students enrolled in WA public schools in grades 3 – 5 during the 2015-16 school year, or all dual credit participants who graduated from WA public high schools during the 2017 school year.)

10. Please describe your study design, methods, and planned analysis (1,500 characters max). If necessary, use the Individual Data Table linked in #11 or a separate document for equations or other important details.

### Requested Data

11. What specific data elements are you requesting, and for what time periods or cohorts? Complete the [ERDC Individual Data Table](#) to help ERDC understand how you would like the data structured (e.g., specific demographics and date ranges, semesters, school years, graduating classes, etc.). **Note: Data requests for a substantial number of variables, cohorts, or records may require more scrutiny from ERDC and a lengthier IRB process.**

### External Data

12. Will you provide ERDC with any other data to link or combine with the data you have requested in your Individual Data Table?

☐ Yes (If so, please explain below, including the number of records that ERDC would need to link.)

☐ No

## Appendix B: Sample Data Sharing Agreements, Privacy Notices, and Data Request Forms

### Contact with ERDC's Partnering Data Contributors

13. Have you consulted with any of the [ERDC's partnering data contributors](#) about your study questions, rationale, or design? ☐ Yes ☐ No  
(Explain below.)

### Timeline

14. What's your ideal date to receive the requested data?

**Note:** ERDC follows a rigorous process for reviewing data requests, as outlined on our [website](#). The time it takes ERDC to review and fulfill a request depends on factors like the complexity of the data, external matching needs, legislative requirements, and the availability of internal data sources. Please allow ERDC at least six (6) months to review and (if approved) fulfill your request.

### Requester's Certification and Signature (Check boxes below)

- ☐ ERDC is required to review **any and all draft materials** (e.g., research reports, scholarly journal publications, presentations, and/or data dashboards) to ensure they comply with FERPA. ERDC must also send the draft materials to data contributors for their review and feedback. **I will submit all draft materials that use the data requested in this form to ERDC for review before any materials are shared with anyone not listed in the data-use agreement and before any materials are published. I will provide ERDC and data contributors with at least ten (10) business days to review the draft materials.**
- ☐ If any part of the draft material is not FERPA-compliant based on the reviews conducted by ERDC and ERDC data contributors, then I will edit the material accordingly to make it FERPA-compliant.

Requester #1's Signature	Title	Date
--------------------------	-------	------

Requester #2's Signature	Title	Date
--------------------------	-------	------

### E-mail the following documents to the [ERDC Inbox](#):

- ☐ Individual Data Request Form
- ☐ Individual Data Table

**Thank you for your submission! ERDC will connect with you after reviewing your request.**

## Acronyms

---

ACCESS NYC	Portal for New Yorkers to screen for benefit and program eligibility
ACF	Administration for Children and Families (Department of Health and Human Services)
AFCARS	Adoption and Foster Care Analysis and Reporting System
AFDC	Aid to Families with Dependent Children
ATM	Automated Teller Machine
CAPTA	Child Abuse Prevention and Treatment Act
CCDBG	Child Care and Development Block Grant
CCDF	Child Care and Development Fund
CCWIS	Comprehensive Child Welfare Information System
CHIP	Children's Health Insurance Program
COTS	Commercial Off-the-Shelf
CP	Custodial Parent
CSP	Cloud Service Provider
CWPM	Child Welfare Policy Manual
ECDC	Early Childhood Data Collaborative
ECE	Early Care and Education
FCR	Family Case Registry
FERPA	Family Educational Rights and Privacy Act
FFPSA	Family First Prevention Services Act
FIDM	Financial Institution Data Match
FISMA	Federal Information Security Modernization Act
FNS	Food and Nutrition Service (Department of Agriculture)
FPLS	Federal Parent Locator Service
HHS	Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
IEVS	Income and Eligibility Verification System
IM	Information Memorandum
IRS	Internal Revenue Service (Department of the Treasury)
IT	Information Technology
LIHEAP	Low Income Energy Assistance Program
MFA	Multifactor Authentication
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
MSFIDM	Multistate Financial Institution Data Match
NCANDS	National Child Abuse and Neglect Data System
NCP	Noncustodial Parent
NDNH	National Directory of New Hires
NIST	National Institute of Standards and Technology
OCSE	Office of Child Support Enforcement (Administration for Children and Families)
OMB	Office of Management and Budget
OPRE	Office of Planning, Research, and Evaluation (Administration for Children and Families)
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
QIC	Quality Improvement Center
QRIS	Quality Rating and Improvement Systems
Q RTP	Qualified residential treatment program
RECS	Residential Energy Consumption Survey
RPG	Regional Partnership Grants
SACWIS	Statewide Automated Child Welfare Information Systems
SAVE	Systematic Alien Verification for Entitlements
SDNH	State Directory of New Hires
SNAP	Supplemental Nutrition Assistance Program (Department of Agriculture)
SORN	System of Records Notice
SPLS	State Parent Locator Services
SSA	Social Security Act
SSI	Supplemental Security Income
SSN	Social Security Number
SSO	Single Sign-On
TANF	Temporary Assistance for Needy Families
TDC	TANF Data Collaborative
UI	Unemployment Insurance
USDA	Department of Agriculture
VPN	Virtual Private Network



# Glossary

---

Term	Definition
Access Control	The technical means used to control who can access an information technology resource.
Audit Control	A technical safeguard that organizations implement as an automated means to record activity in an information system.
Biometrics	Body measurements and calculations related to human characteristics used for authentication in computer science as a form of identification and access control.
Clearinghouse	A place for the exchange of information concerning a specific topic.
Consent	Voluntarily giving agreement or permission for something to happen; such as the use of one's personal information.
Data Collaborative	A collaboration among participants from different sectors to exchange their data to create public value.
Data Confidentiality	The status accorded data indicating that they are protected and must be treated as such. (Source: <i>Health Data in the Information Age: Use, Disclosure, and Privacy</i> . Institute of Medicine, National Academy Press, 1994.)
Data Exchange Standards	Establish a common set of definitions, and the structure and format of key variables, setting a foundation for sharing data across data sources.
Data Privacy	Focuses on compliance with data protection regulations; how data should be collected, stored, managed, and shared to protect privacy of individuals. It is a state or condition of controlled access to personal information. It is the right of a citizen to have control over how personal information is collected and used. (Source: Emotive website, Glossary web page, and <i>Health Data in the Information Age: Use, Disclosure, and Privacy</i> . Institute of Medicine, National Academy Press, 1994.)
Data Security Agreement	A document that governs privacy and security of data.
Data Sharing Agreement	A document that governs the sharing or transferring of data.
De-identified Information	Data that remain after any personally identifiable information has been removed.

Term	Definition
Digital Signature	One of two methods for electronically recording an individual's consent to share his or her information; a digital signature is issued to an individual by a company or application that runs a certificate authority.
Direct Identifying Information	Data that directly identifies a single individual, such as names and Social Security Numbers. (Source: NISTIR 8053, <i>De-Identification of Personal Information</i> , Simon L. Garfinkel, National Institute of Standards and Technology, Oct 2015.)
Electronic Interface	A shared boundary across which two or more separate components of a computer system exchange information.
Electronic Signature	One of two methods for electronically recording an individual's consent to share his or her information; an electronic signature is a sound, symbol, or process that gets placed on a document, file, or item by a person with intent to sign.
Encryption Certificate	A certificate-based system that works with the web server and web browser to encrypt the flow of information between them.
Horizontal Data Integration	A method of uniting information of the same type, but from different data sources and, potentially, in different formats.
Income and Eligibility Verification System	Federal regulations require states to conduct automated data exchanges to verify client eligibility and proper amounts of benefits.
Indirect Identifying Information	Information that can be used to identify an individual through association with other information. (Source: NISTIR 8053, <i>De-Identification of Personal Information</i> , Simon L. Garfinkel, National Institute of Standards and Technology, Oct 2015.)
Integrated Case Management	A case management approach that enables health and human services organization staff to access centralized client records, comprehensive service delivery history, and concurrent case activity information to improve outcomes of the families it serves.
Interoperable Standards	Used to provide a common language and a common set of expectations that enable interoperability between systems and/or devices.
Interoperability	The property that allows for the unrestricted sharing of resources between different systems (i.e., technological and programmatic coordination).

Term	Definition
Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)	An MOU is a legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. An MOA is a document written between parties to cooperatively work together on an agreed upon project or meet an agreed upon objective. It can also be a legal document that is binding and hold the parties responsible to their commitment or just a partnership agreement. (Source: University of Alaska Southeast website, Administrative Services webpage.)
Microdata	Information gathered at the level of the individual from data sources that may include, surveys, administrative data, census data, marketing data, and unstructured data such as from social media.
Personally Identifiable Information	Any data that could potentially identify a specific individual, or distinguish one person from another, or can be used for de-anonymizing previously anonymous data. These data include direct identifying information and indirect identifying information.
Program Integrity	Improving stewardship of public funds by reducing fraud, ensuring accurate eligibility determinations, and reducing improper payments.
Re-identification	A general term for any process that re-establishes the relationship between identifying data and a data subject. (Source: NISTIR 8053, <i>De-Identification of Personal Information</i> , Simon L. Garfinkel, National Institute of Standards and Technology, Oct 2015.)
Statutory Authority	Refers to the powers and duties assigned to a government official or agency through a law passed by Congress or a state legislature.
System of Records	A group of records under the control of a federal agency from which information is retrieved by the name of the individual or some other identifier assigned to the individual.
System of Records Notice	A notice in the Federal Register that describes a system of records.
User Authentication	Verification of user's identity, and confirming they are authorized to access the specific data requested.