

---

# Confidentiality Toolkit

---

A resource tool from the  
ACF Interoperability Initiative

This page intentionally left blank.

# Preface

---

We're very pleased to be issuing the Administration for Children and Families (ACF) Confidentiality Toolkit, a product of ACF's Interoperability Initiative.

For decades, human services agencies have been seeking to identify ways to promote coordination and collaboration across the work of human services and other related entities in order to provide more effective services to children, families, and individuals with multiple needs.

In recent years, advances in technology have provided new opportunities to support these efforts. "Interoperability"—a national effort of technological and programmatic coordination—has the potential to provide for major steps forward in promoting information sharing and coordination across systems. For that reason, we created the *ACF Interoperability Initiative Project*, a collection of collaborative, interdisciplinary information technology projects designed to promote horizontal integration, facilitate shared services, and improve the landscape of systems supporting human services programs, including their coordination and integration with health programs.

As states are developing Health Insurance Exchanges and new eligibility systems for Medicaid, there is an opportunity for Human Services programs to utilize components and services provided by these new systems. But having new systems alone isn't a panacea. Systems need data. And, the ability to share information across systems will be crucial to the success of these efforts.

At the same time, improved information sharing is not simply a technological challenge. 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, e.g., domestic violence programs, confidentiality provisions may literally be life-saving. 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.

While confidentiality provisions play a vital public purpose, it is also the case that too often the complexities resulting from multiple varying confidentiality provisions can be a significant impediment to state and local efforts to improve service coordination. This can occur because it is sometimes unclear 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.

With publication of this, our ACF Confidentiality Toolkit, we hope to support state and local efforts by bringing greater clarity to the rules governing confidentiality in ACF and certain related programs, by providing examples of how confidentiality requirements can be addressed and met in a manner fully consistent with governing laws and underlying policies; by including sample

Memoranda of Understandings and data sharing agreements; and by providing guidance that we hope can be helpful in efforts to move forward in states and localities.

We recognize that we are not addressing all programs and every potential issue, but we hope that this Confidentiality Toolkit will be helpful in state and local efforts, and we welcome your comments and suggestions for additional guidance and actions by ACF and other federal partners that can further support these efforts.

Many dedicated people assisted in conceptualizing, researching, and reviewing this Confidentiality Toolkit. We appreciate the work of Joe Bodmer of the Office Child Support Enforcement for directing our ACF Interoperability Initiative and for bringing this toolkit together. Thanks go out to Carli Wulff for her efforts in coordinating final review across ACF offices, and to the Stewards of Change led by Daniel Stein for the initial research and work on the toolkit. We also want to thank all six human service programs that contributed to and helped edit the toolkit. And finally, we want to thank our colleagues at the American Public Human Services Association who have highlighted the need for efforts such as this one for a number of years.

Mark Greenberg  
Acting Assistant Secretary  
Administration for Children and Families

# Table of Contents

---

Preface .....	3
Table of Contents.....	5
Chapter 1. Introduction .....	10
The Case for Sharing .....	10
Purpose of the Toolkit.....	11
Organization of the Toolkit.....	12
Individual Chapters .....	12
Program Matrices.....	12
Memorandums of Understanding.....	12
Getting Started .....	12
Policy Development.....	13
Staff Development .....	14
Legal Development.....	15
Chapter 2. Child Welfare.....	16
The Case for Sharing .....	16
Applicable Federal Legislation .....	17
Child Abuse Prevention and Treatment Act (CAPTA).....	17
Child and Family Services Improvement and Innovation Act.....	19
Fostering Connections to Success and Increasing Adoptions Act.....	20
Statewide Automated Child Welfare Information Systems (SACWIS).....	21
Title IV-E of Social Security Act, Payments for Foster Care and Adoption Services .....	21
Title IV-B of the Social Security Act, Child and Family Services .....	23
Family Educational Rights and Privacy Act (FERPA) and the Uninterrupted Scholars Act (USA).....	24
Implementation: What and Who.....	25
The Program Group.....	26
The Legal Group.....	26
Implementation: How.....	27
Court Order .....	27

State Statute.....	27
Major Federal Laws and Regulations .....	27
Chapter 3. Temporary Assistance for Needy Families (TANF).....	29
The Case for Sharing .....	29
Applicable Federal Legislation .....	30
Title IV-A of the Social Security Act, Temporary Assistance for Needy Families.....	30
Implementation: What and Who.....	30
The Program Group.....	30
Implementation: How.....	31
The Legal Group.....	31
Major Federal Laws and Regulations .....	31
Chapter 4. Child Support.....	32
The Case for Sharing .....	32
Applicable Federal Legislation .....	33
Title IV-D of the Social Security Act, Child Support Enforcement .....	33
Implementation: What and Who.....	33
The Program Group.....	34
Implementation: How.....	34
The Legal Group.....	34
Major Federal Laws and Regulations .....	35
Chapter 5. Child Care.....	36
The Case for Sharing .....	36
Applicable Federal Legislation .....	36
Child Care and Development Block Grant.....	36
Implementation: What and Who.....	37
The Program Group.....	38
Implementation: How.....	38
The Legal Group.....	38
Major Federal Laws and Regulations .....	39
Chapter 6. Low-Income Home Energy Assistance Program (LIHEAP).....	40
The Case for Sharing .....	40
Applicable Federal Legislation .....	40

Home Energy Grants .....	40
Implementation: What and Who .....	40
The Program Group .....	41
Implementation: How .....	41
The Legal Group .....	41
Major Federal Laws and Regulations .....	41
Chapter 7. Supplemental Nutrition Assistance Program (SNAP) .....	42
The Case for Sharing .....	42
Applicable Federal Legislation .....	43
Food Stamp Act of 1964, as amended, now known as the Supplemental Nutrition Assistance Program (SNAP) .....	43
Implementation: What and Who .....	44
The Program Group .....	44
Implementation: How .....	45
The Legal Group .....	45
Major Federal Laws and Regulations .....	45
Chapter 8. Information Technology Support To Confidentiality .....	46
The Case for Sharing .....	46
Enabling Information Sharing .....	46
Enabling Efficient Sharing .....	47
Enabling Confidential Sharing .....	48
Access Control .....	48
Audit Control .....	49
Integrity and Transmission Security .....	50
Enabling Shared Understanding .....	51
Conclusion .....	52
Appendix A – Matrices .....	53
Matrix One. Child Welfare .....	53
Matrix Two. Temporary Assistance for Needy Families .....	61
Matrix Three. Child Support .....	64
Matrix Four. Child Care .....	71
Matrix Five. Low Income Home Energy Assistance Program (LIHEAP) .....	74
Matrix Six. Supplemental Nutrition Assistance Program (SNAP) .....	75

Appendix B - Memorandums of Agreement and Understanding, Security Agreements, and Notices of Privacy Practices ..... 85

State of Kentucky – Memorandum of Agreement ..... 85

State of New York – Master Memorandum of Understanding ..... 91

State of Colorado – Master Memorandum of Understanding ..... 95

ACF/Office of Child Support Enforcement – Security Agreement ..... 98

Montgomery County, Maryland – Notice of Privacy Practices ..... 120

Glossary of Terms ..... 127

---



**DISCLAIMER:** This toolkit is not intended to be relied upon as 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.

# Chapter 1. Introduction

---

## The Case for Sharing

**C**onfidentiality and privacy have long been keystones of our society. With the advent of electronic and computer technologies, sharing and accessing information became easier and, at the same time, our ability to protect confidentiality and privacy is greatly enhanced. Concurrently, legitimate concerns have arisen about data security and the tremendous potential for unauthorized sharing of personal information. Federal and state statutes and regulations were put into place to protect privacy and confidentiality. Although these rules were put into place to protect individuals, sometimes these rules make it difficult to achieve broader goals to help individuals and families that can best be advanced by sharing information among multiple programs.

Today, persons receiving governmental services are often involved with multiple systems. A young mother and her child may receive income assistance, SNAP benefits, child care and child welfare services, mental health and drug or alcohol treatment services, or other federally-supported programs. Each of these services were designed to fill a distinct purpose, with each requiring different data and following different rules and requirements. This approach does not always support effectiveness and efficiency. Coordinated care and integrated case management can improve the overall health and well-being of individuals. Better outcomes mean healthier, safer, stabilized individuals and families with a better chance of sustaining self-sufficiency and long-term

personal success, which, in turn, reduces costs to the state and local governments.

As human service providers, we must find balanced approaches that promote information sharing, protect confidentiality and privacy, increase data security, improve services and outcomes, increase efficiency, and reduce duplication of efforts for both clients and the workforce. Jurisdictions would be remiss to not take advantage of the tremendous technological advances of this decade to improve outcomes and efficiency for both clients and staff where statutory and regulatory authority exists.



It is impractical for individual case workers or managers from different systems to reach agreement about information sharing for the individual client but these types of arrangements may be possible between systems. Change is occurring across the country as leaders from health and human service agencies at the state and local level

step forward and establish a culture of openness to collaboration.

The Administration for Children and Families (ACF) developed this *Confidentiality Toolkit* to help jurisdictions successfully navigate the delicate balance between privacy and security with the delivery of efficient and effective services. The Confidentiality Toolkit analyzes, explains and aids 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 and sample documents from across the country from which jurisdictions using the Toolkit can borrow freely.

This Toolkit has been developed for leaders in the human service field, to support their best efforts to share information across silos.

### **Purpose of the Toolkit**

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. Policy, including program development and review; and,
3. Program evaluation, performance measurement, and research.

The Toolkit addresses information sharing for the purpose of individual case planning and decision-making at a program level. Such information must be case-level and identifiable. Aggregated and de-identified information is helpful for policy and program development, but may not be helpful in a particular case where the case manager is developing a specific individual's service plan.

This guide is also intended to help **human service administrators and other professionals** navigate intersecting laws. Agency directors can use this Toolkit to initiate a data sharing dialogue with directors from other systems and agencies. Although agency and system directors may sometimes have the perception that federal law prohibits information sharing, that perception is often incorrect.

The Toolkit is a road map intended to help get to the answer of “yes.” With the Toolkit, **states and counties** can learn to share important information so that human services agencies can more effectively serve clients and more efficiently allocate resources. It will enable **states and local jurisdictions** to determine ways to share necessary information and, at the same time, protect peoples' rights to confidentiality and privacy.

With the Toolkit as a guide, **states and localities** can facilitate better information collection and sharing across our human service programs and systems, while at the same time protect individuals' rights to confidentiality and privacy. **States** will be more able to clarify in their own policies and processes the access to information and client notification regarding the storage, use, reuse, sharing, and client correction or updating of information.

The Toolkit does not replace the important process of consulting with your own legal counsel. But hopefully, for those interested in using data sharing to support their mission, we have outlined in the tables contained in this document a clear vision of what is permissible and, importantly, where no federal instruction exists. This Toolkit will enable leaders to proceed in an organized, efficient and effective manner.

## Organization of the Toolkit

The Toolkit as a whole contains:

- Individual chapters addressing confidentiality and privacy through the lens of particular areas of service provision: Child Welfare, Child Care, Temporary Assistance for Needy Families (TANF), Child Support, Low Income Home Energy Assistance Program (LIHEAP), and the Supplemental Nutrition Assistance Program (SNAP);
- Reviews of federal laws and regulations regarding Child Welfare, TANF, Child Support, Child Care, LIHEAP, and SNAP. For each law, the Toolkit



provides a basic, understandable description of the confidentiality issues. It highlights the law's specific language permitting information sharing and outlines the information and practical and usable definitions of the data elements where necessary;

- An appendix with matrices, by program, of applicable federal laws; and,
- A second appendix with memorandums of understanding addressing data sharing from Kentucky, New York, Colorado, the Office of Child Support Enforcement, and Montgomery County, Maryland.

## Individual Chapters

In specific chapters, several questions are posed and answered:

- What information can be shared?
- Why is it necessary to share the information?
- What is the best method for information sharing?
- Who can receive the information?
- How will those receiving the information maintain its confidentiality and protect it from further disclosure?

## Program Matrices

The first appendix contains matrices for each of the six programs described herein. The matrix for each program attempts to tie back to specific legislative authorities, the data sharing opportunities, and the applicable programs that personally identifiable information and data can be shared.

## Memorandums of Understanding

A second appendix provides five excellent examples of memorandums of understanding and data security agreements governing privacy and security of data that is shared.

Where necessary and outside of the scope of this document, but throughout the Toolkit are helpful references to other tools and writings to best equip states and localities for the journey ahead.

## Getting Started

This section provides **state and local human service leaders** with a brief overview of the steps required to develop information sharing plans to improve outcomes for clients,

increase efficiency of operations, and protect the confidentiality rights of individuals. This undertaking will require a significant investment of time and effort from many people. It will also require an unwavering leadership commitment. Necessary participants for this effort are:

- Top leaders of the different systems, convening groups to set the tone and direction, developing a privacy policy and then using the dictates of that policy to reach a Memorandum of Understanding (MOU) regarding the information sharing process;



- Lawyers to determine how to legally protect the confidentiality and privacy issues;
- Technology personnel determining the most cost-effective manner of sharing the information;
- Security officers verifying the recipients of the information and ensuring ongoing data safety; and,
- Last, and of paramount importance, program experts from the policy, operational and practice areas, to determine the specific information to be shared to achieve better outcomes for the clients.

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

- Take the lead in the development of any and all MOUs and cross-agency information sharing documents;
- Designate a team of staff, from the areas of services that are being planned, to create the “**what**,” or list of minimally necessary information needing to be shared for the legitimate governmental purpose to succeed, and the “**who**” that needs to receive such information;
- Designate a team, including the privacy officials and the information technology staff, to determine “**how**” to share the information and protect it once shared. This group also will 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 extensive training of all members of the workforce on the policies and procedures regarding the information sharing project once it is initiated and fully implemented; and,
- Arrange for the crafting of policies and procedures regarding appropriate safeguards for sharing.

The process moving forward can be divided into three areas: policy development, staff development, and legal development.

### Policy Development

Policy Development answers the “**why**” question. Why should systems share information when they never have shared in the past? Why now? Two documents need to be developed to provide the answers:

- A statement of “shared vision” providing the reason for the information sharing initiative. Greater information sharing (properly executed, of course) will have benefits for all stakeholders and sectors – through improved service and outcomes, enhanced customer access, and more efficient and less costly administration. The vision cannot be “shared” unless all parties understand how they will benefit from changing their orientation toward these broad outcomes rather than defending what has been formerly seen as individual lines of business and subsequent information that cannot be changed or shared with “outsiders”; and,
- A document—an MOU or a Memorandum of Agreement (MOA)—outlining the information to be shared, how the information will be shared, and the protections of the information once shared. (References of “shared visions” and memorandums are either referenced or copies are included in this Toolkit.)

Along with the actual documents, the process to create these documents is also important, so included samples should not be viewed as shortcuts to the real collaboration required. When systems are developed and have functioned separately from other systems, there may be a lack of knowledge about each other. Each program’s system understands its own process of security and protecting information, but one system may not know the governing policies, procedures, laws and regulations of another program’s system. There may be a lack of trust between practitioners of different programmatic areas and their systems that can only be overcome through sustained collaboration over time. Building trust takes time. It must be an inclusive process involving the different levels

and roles within the agency to provide input on the importance of information sharing, the ways data sharing could improve job performance, and the specific information required to accomplish this mission. Used inclusively, this process will build valuable agreement and agency-wide ownership.

The public and the advocates should also be kept informed during the process, to address any concerns that the ease of data sharing, through electronic information technology, will erode all rights of confidentiality and privacy. It is leadership’s role to be clear with the client population, advocates, the legislature, the providers and practitioners, the other system partners, and the public that this project will include a thorough review of privacy and confidentiality issues and that these rights will be acknowledged and protected. Engagement of advocates in the process can ensure that confidentiality issues are fully addressed and that there is broad shared consensus on how best to move forward. It is also important to make clear that the information technology will aid in this process by securely maintaining and protecting any data involved.

Throughout, it will be important to share information on progress with all of concerned constituents to ensure the project’s transparency and avoid or significantly decrease fears about the sharing of an individual’s personal information.

### **Staff Development**

As part of any information sharing initiative, it is essential for the staff, at all levels of the involved systems, to meet to decide “**what**” information is minimally necessary to be shared in order to accomplish the mission. This is an essential and challenging part of the

process because the group must be very selective and specific. If the information is not necessary, then it should not be shared. Too little information is not useful and too much information is equally useless. While often frustrating, it is worth the effort. This group should also search to see whether other jurisdictions have shared similar information to understand how they accomplished the task and learn about successes to follow and pitfalls to avoid.

In addition to “**what**” information is necessary, this group needs to determine “**who**” needs the information. This part of the process will identify the staff persons or classes of persons—and the supervisory chain—requiring access to the shared, protected 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 conduct a careful review to determine whether the shared information is necessary to perform essential functions.

### **Legal Development**

The role of agency lawyers in information sharing initiatives is to provide legal and statutory interpretation, protection, and critical information on accomplishing the set of goals. Leadership in all involved agencies must make clear to their legal staffs that they want to share the information, that it is an important initiative, and that the agencies need the lawyers to help make it happen. Lawyers must also make sure that individuals’ rights to privacy and confidentiality are upheld. Therefore, for any barrier identified, the legal group must also seek to present suggestions to overcome the barrier. The process should include reviewing federal, state, and local laws as relevant to determine

any barriers or requirements for information sharing. The explanation and discussion must be understandable to the layperson and not only to other lawyers.

The legal group’s accomplishments must also include drafting appropriate notices of 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 required language translations that may be required.

## Chapter 2. Child Welfare

---

### The Case for Sharing

Child abuse and neglect has been shown to have lifelong adverse health, social, and economic consequences. These consequences include behavioral health conditions, behavioral problems, delinquency and adult criminal activities, violent behavior, increased risk of chronic diseases, disability from physical injury, reduced health-related quality of life, and lower levels of adult economic capacity and are also associated with large societal costs.<sup>1 2</sup>

Children and youth in foster care are very often involved with multiple systems and present complicated issues in addition to achieving normal development in childhood, and adolescence. To ensure the safety and well-being of children in foster care, all stakeholders must have current and accurate information regarding the subject 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 juvenile justice. Access to current, accurate information helps ensure that situational-appropriate services can be delivered in a

timely fashion to children in foster care. In reviewing all current federal child welfare laws, most of the applicable statutes recognize the need for information sharing by the child welfare system with other systems and encourages or mandates that systems work together to increase successful outcomes for children and youth in foster care.

There are a number of 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. One way to share this information is to provide a secure exchange between systems, as in the following examples:

- TANF/Medicaid systems, to facilitate a child's eligibility determination for title IV-E foster care maintenance payments;
- Schools to facilitate school stability and education 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;
- The juvenile justice system to improve coordination between both the child welfare case worker and the probation officer;
- The mental health system on mental health services provided to the child to coordinate on the child's treatment; and,

---

<sup>1</sup> Fang, X., et al., "The economic burden of child maltreatment in the United States and implications for prevention," *Child Abuse & Neglect* (2012).

<sup>2</sup> Fang, X., et al. Using an incidence-based approach, the study estimates the average life cost per victim of child abuse/child neglect to be \$210,012 for non-fatal victim and \$1,272,900 for fatal victim, for a total cost of \$124 billion as of 2008.



- Drug and alcohol treatment systems on treatment services to an addicted child, and to the addicted parent for permanency purposes.

### Applicable Federal Legislation

Included in this section are key provisions of federal child welfare laws and how each supports information sharing with other systems. With the understanding that none of the federal child welfare laws ban information sharing, the laws protect the rights of the children and families involved with child welfare systems and in some cases limit the

*ACF, the Center for Medicare and Medicaid Services (CMS), and the Substance Abuse and Mental Health Services Administration (SAMHSA) issued a joint letter on November 23, 2011 to all state directors to encourage them to strengthen their systems of prescribing and monitoring the use of psychotropic medication among children in foster care. This joint letter was followed by a two-day working group that convened on August 27 and 28, 2012, called: "Because Minds Matter: Collaborating to Strengthen Management of Psychotropic Medications for Children and Youth in Foster Care."*

*The meeting brought together representatives from state child welfare, Medicaid, and mental health systems from all fifty states, the District of Columbia, and Puerto Rico, as an opportunity for state leaders to enhance cross-system efforts ensuring appropriate use of psychotropic medications and to discuss state-of-the-art information on cross-system approaches for improving mental health and well-being.*

dissemination of sensitive information and case-specific details.

The following reviews the federal child welfare laws and the legal authorities that protect information sharing and privacy related to child welfare.

### Child Abuse Prevention and Treatment Act (CAPTA)

CAPTA is one of the key pieces of federal legislation that guides child protection, as well as prevention and treatment of child abuse. These requirements apply to CAPTA grants and as part of the Act, HHS is to consult with other federal agencies that operate clearinghouses and to consult with such departments for sharing information involving child abuse and neglect. Key components of CAPTA related to confidentiality and information sharing include:

- Requiring that, as a condition of receiving a CAPTA State grant, a State assure that it is operating a program 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, including other entities who are authorized by statute to receive information pursuant to a legitimate State purpose.
- Requiring that, per section 106(d) of CAPTA, all states that receive a CAPTA state grant provide, to the extent practicable, an annual state data report to HHS, including data regarding the incidence of child abuse and neglect.

- 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, including methods of continuity of treatment planning and services.
- Requiring HHS to provide technical assistance to states, and provides that this technical assistance may include an evaluation of approaches to enhancing the linkages between child welfare agencies to coordinate the provision of services with health care agencies, alcohol and drug abuse treatment and prevention services, education institutions, and mental health agencies. CAPTA also allows HHS to provide grants to states for training to enhance linkages and to entities that provide linkages among child protective service agencies and health care agencies, entities providing physical and mental health services, community resources, and developmental disability agencies. In addition, states may 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.
- Permitting HHS to award demonstration grants to develop a triage system that may include innovative partnerships in responding to reports of child abuse and neglect with law enforcement and developmental disability agencies, and substance abuse treatment, health care, domestic violence prevention, and mental health services entities.

- Allowing states to use CAPTA state grants to create and improve multidisciplinary teams and interagency protocols to enhance investigations.

CAPTA does not prohibit information sharing. In general, 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. However, CAPTA allows the state to release information to certain individuals and entities.

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 (section 106(b)(2)(B)(viii)(I));
- A grand jury or court, when necessary to determine an issue before the court or grand jury (section 106(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 (section 106(b)(2)(B)(viii)(VI)).

In addition, states have the option to allow public access to court proceedings that determine child abuse and neglect cases, so long as the state, at a minimum, can ensure the safety and well-being of the child, parents and families (see the last paragraph of section 106(b)(2) of CAPTA).

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

*In Ventura County, California, recognizing the complex health and care needs of children in foster care, the county successfully piloted “Foster Health Link”, a public-private joint effort to use the potential of information technology to improve the health outcomes for this population. The electronic system links existing independent data systems and produce summary records of health needs and conditions for individual children living in foster care. The electronic system links existing independent state and county data systems used separately by caseworkers and health providers and enables the generation of summary records of health needs and conditions of individual children living in foster care while maintaining essential privacy protections.*

to protect children from abuse and neglect (permitted by 106(b)(2)(B)(viii)(II) but required by section 106(b)(2)(B)(ix));

- Child abuse citizen review panels, if such panels are established to comply with section 106(c) of CAPTA (permitted by 106(b)(2)(B)(viii)(III) but required by section 106(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 section 106(b)(2)(B)(x)), in accordance with section 2.1.A.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 section 106(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. There may be other federal confidentiality restrictions for the state to consider when implementing the confidentiality provisions under CAPTA.

### **Child and Family Services Improvement and Innovation Act**

Among other provisions, this law (section 437(f) of title IV-B) allows HHS to award grants to regional partnerships that provide integrated activities and services that are designed to increase the safety, permanency and well-being of children who are in an out-of-home placement as a result of a parent’s or caretaker’s substance abuse.

In addition, data collected under title IV-B of the Act must be made interoperable. To accomplish this transformation, electronic data exchanges of IV-B information between systems must incorporate interoperable standards developed and maintained by intergovernmental partnerships, such as the National Information Exchange Model (NIEM). Though these standards require implementing regulations which have not yet been written, it is important to note the statutory recognition and importance placed on interoperability by this Act.

### Fostering Connections to Success and Increasing Adoptions Act

The Fostering Connections Act primarily amended title IV-E of the Act by placing specific mandates on child welfare agencies for education stability, health oversight and coordination, and transitional planning for children and youth in foster care. Under Fostering Connections, the state and/or tribe must:

- Ensure educational stability for a child while in foster care, including assurances that a child’s placement takes into account the appropriateness of the current educational setting and the proximity of the placement to the school in which the child is enrolled at the time of placement;
- Coordinate with appropriate local educational agencies to ensure that the

records of the child provided to the school; and,

- With other systems, including the state’s Medicaid agency, develop a plan for ongoing oversight and coordination of health services for children in foster care. This includes a coordinated strategy to identify and respond to physical, mental, and dental health needs.<sup>3</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.
- For every child in foster care attaining the age of 18 years of age, during the 90-day period immediately prior to that birthday, provide a transition plan through case management services and with assistance and direction by the youth. Plans must include specific options on housing, health

*On August 1, 2012, OCSE and the Children’s Bureau issued a joint Information Memorandum (IM-12-06) that provides information on how State child support and child welfare agencies can improve their work, including through electronic data exchanges between child welfare and child support information systems. The Information Memorandum discusses the child support agency’s authority to share certain information about parents and relative, including location information, from the Federal Parent Locator Service (FPLS) and the State Parent Locator Service (SPLS) with the state child welfare agency. The Information Memorandum clarifies the specific information that it can share with the state child welfare agency when locating a relative for title IV-B/IV-E program purposes. It also provides examples of appropriate referrals and inappropriate referrals from the child welfare agency to the child support agency. Last, the document encourages the two state agencies to automate location requests and share necessary case information to carry out their mutual system responsibilities.*

child remains in the school in which the child is enrolled at the time of the placement or, if remaining in such school is not in the best interests of the child, immediate and appropriate enrollment in a new school with all of the educational

<sup>3</sup> Specifications of plan are included in law—initial and follow-up health screenings, how health needs identified are treated and monitored, how medical information is updated and appropriately shared, steps to ensure continuity of health care services, oversight of prescription medicines, and active consultation with and involving physicians and other appropriate medical and other professionals in assessing health and well-being.

insurance, education, continuing support services, work force supports and employment services.

To assist state child welfare agencies in carrying out their responsibilities, the Fostering Connections Act requires the federal Office of Child Support Enforcement (OCSE) within the U.S. Department of Health and Human Services, to provide state child welfare agencies with access to information contained in the Federal Parent Locator Service.<sup>4</sup> OCSE has promulgated a rule and is partnering with the Children's Bureau and state child welfare agencies to implement this provision.

### **Statewide Automated Child Welfare Information Systems (SACWIS)**

To avoid duplication of effort and achieve maximum use of first-hand information regarding children in foster care and their families, all child welfare information is to be directly entered into the SACWIS for each state that has such a system. Other agency workers with shared cases or title IV-E eligible cases can download or enter information directly into the SACWIS. It also provides for interfaces with other automated information systems including but not limited to court and juvenile justice systems, vital statistics, child support, and education.

The Act and/or implementing regulations at 45 CFR 1355.53(b)(2) states that, to the extent practicable and appropriate, the state should provide for electronic exchanges and referrals with other data collection systems including TANF, Medicaid, child support, and the National Child Abuse and Neglect Data System (NCANDS). At the same time, it does not specifically discuss interoperability

<sup>4</sup> 42 U.S.C. 653(j)(3).

or incorporating interoperable standards developed and maintained by inter-governmental partnerships.

### **Title IV-E of Social Security Act, Payments for Foster Care and Adoption 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 the 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 provides federal reimbursement to states and tribes for adoption assistance, and at state/tribal option, kinship guardianship assistance payments.

*In partnership with a large managed care organization serving the majority of children in foster care in Allegheny County, Pennsylvania, the Allegheny County Department of Human Services and the University of Pittsburgh Medical Center (UPMC) created an electronic E-Health Record for this population. The information is shared with the caseworkers.*

States must coordinate programs under title IV-E with programs under TANF, 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:

- Exceptions to use individual information include: TANF, Child and Family Services, child support, 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;
- Exception for criminal and civil proceedings and law enforcement when in connection with the administration of one of the aforementioned programs;
- Exception 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; Exceptions for reporting and providing information to appropriate authorities with respect to known or suspected child abuse or neglect; and,
- Exception 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.

Educational, health, special needs and transition from foster care requirements of the statute include:

- States 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 name and address of education

provider, grade level performance, and school record;

- Educational stability requirements for children in foster care, including assurances that 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;
- Assurance of collaboration with appropriate local educational agencies to ensure that the child in foster care remains in the school in which the child is enrolled at the time of placement, or if remaining in such school is not in the best interests of the child, assurances by state child welfare

*A request was made for a state's SACWIS to have access to the food stamp program file information. The state SACWIS system had sought but was denied access to this information. The U.S. Department of Agriculture (USDA) made clear that regulations permit disclosure of this information to "federally-assisted state programs providing assistance on a means-tested basis to low income individuals." It further found that the child welfare programs qualify as such and therefore the food stamp file information may be permitted to be shared with SACWIS.*

and educational agencies to provide immediate and appropriate enrollment in a new school, with all of the educational records of the child provided to the new school;

- Determination of "special needs" for an applicable child under title IV-E adoption assistance program if a child is receiving

SSI benefits under title XVI of the Act and meets the other two prongs of section 473(c)(2) of the Act. A 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 such child cannot be placed with adoptive parents without providing adoption assistance or Medicaid under title XIX of the Act, 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 be returned to the home with his or her parents;

- Written health care case plan requirements for children in foster care must include name and address of health care provider(s), and records of a child’s immunizations, known medical problems, medications and any relevant health information; and,
- 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.

As title IV-E addresses confidentiality and privacy, the use or disclosure of information concerning individuals is restricted to purposes directly connected with the administration of the plan, (with a limited set of exceptions as previously discussed), developed by the particular state or tribe under this chapter.

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

The statute provides for the coordination of services using IV-B funds, as well as, funds under 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 CFR 1355.30 (p)(3) records maintained under title IV-B and IV-E of the Act are subject to the confidentiality provisions in 45 CFR 205.50. Among other things, 45 CFR 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 106 of CAPTA. 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;
- The highest court in the state can apply for Court Improvement Program Funds to collect and share relevant information, including descriptions of how courts and child welfare agencies on state and local levels collaborate and jointly plan for the collection and 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.

*In the Travis County, Texas, 98<sup>th</sup> Judicial District Court, the court worked with all of the parties to craft a judicial order format so that the minimum necessary information is ordered to be shared in cases of youth who cross between the child welfare and the juvenile justice systems. The sole purpose for the information sharing and court order is to provide such youth every opportunity to maximize a youth's experience in multiple systems and improve outcomes for these youths, including helping to reduce recidivism, increase reunification and permanency, and increase successful re-entry into society.*

### **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 good and necessary 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, when it comes to education records, the child welfare program is not necessarily in charge. Schools 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 CFR 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. Parents and eligible students (students who have reached 18 or are attending a postsecondary institution at any age) must provide written consent before personally identifiable information (PII) is disclosed from the student's education records. However, there are a number of exceptions to FERPA's general consent rule.

FERPA is sometimes perceived as an obstacle to schools sharing information with child welfare agencies and the courts. But this perception is not necessarily based in fact. While the first step should always be to seek the parent's consent, FERPA has a number of important exceptions to its *general rule*, and many states and localities around the country are successfully sharing educational information for children in care among and across agencies.

FERPA allows "directory information" to be disclosed without parental consent after the school gives general notice to all parents and eligible students of its intent to release 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 to be “directory information” for purposes of allowable disclosure without parental consent.

The Uninterrupted Scholars Act (USA), also referred to as the A+ Act, 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 personally identifiable information (PII) from the 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 (CWA) 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.” *See* 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. *See* 20 U.S.C. § 1232g(b)(2)(B).

Of course there are other important FERPA exceptions, not just the ones authorized by the USA or the exception for disclosing directory information. One such exception authorizes the disclosure of student-specific information from a child's education records when needed to comply with a judicial order or lawfully issued subpoena. Under this exception, for example, a school could disclose 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**

While an MOU is generally recommended, there are few circumstances in which they are required by federal law. However, for a successful information sharing initiative regarding child welfare data, agency heads can agree to an MOU as to the information to be shared, with whom, and by what method. Though many options, as previously discussed, are permissible, to share information on an individual case basis, and depending on the state's particular laws regarding the subject matters, the systems have three primary options:

- An individual court order mandating that information be shared;

- An authorization signed by the legally-recognized individual; and,
- State statute mandating that individual case information is shared to better serve the client and improve outcomes for the population, consistent with federal law.

For successful implementation of 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











As a first step, the program group, consisting of policy and practice experts, should

*In Los Angeles, California, as well as in many other jurisdictions across the country, the Department of Education, and by extension local educational agencies (LEA's) and schools, automatically ask the parents or guardians to sign a "parental consent form" whenever a child is placed in out-of-home care. The form explains to whom the child's education records may be disclosed and that the parents' consent is voluntary.*

determine **what** information is necessary to share, being careful to maintain the balance between data exchange and how much is "too much." The next task for the program group is to determine **who** has access to the information, which is dependent on the

presenting policy and operational reasons for the information sharing process. The access should be based on either the person's responsibilities or the job classification's responsibilities and should be limited to only those persons who "need to know" this information in order to perform their job responsibilities and to further provide and improve services to the youth.

The group's list might look something like this:

-  Name of youth
-  Social Security Number
-  Case Number
-  Participant Identification Number
-  Current Address
-  Contact telephone number
-  Electronic mail address (email)
-  Date and place of birth
-  Personal goals
-  Projected date of discharge from care

### The Legal Group

The first task for the legal group to decide is whether the specific child welfare information is confidential and protected based on federal laws, recognizing that the federal law provides 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, and SSI, and child support. State practices vary widely regarding the amount and type of information that they share with these agencies, based on the unique needs of their state programs and state laws.

In addition, this group should accumulate all of 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

working with the same person. The group must examine each state law to determine how it encourages information sharing to improve outcomes for this population as well as additional specific requirements. For each of the requirements, the legal group must provide suggested vehicles for sharing the information and meeting the requirements.

Examples of protected child welfare information may be the factual information regarding the reasons that the child is in the custody of the state, the mental health, drug and alcohol diagnosis (if maintained by the child welfare agency), history, and treatment of the child, the parent, or others involved with the family, HIV/AIDS, communicable disease information, and possibly the exact placement of the child due to the circumstances of the placement and the danger to the child. If the information is protected, the information sharing options generally to consider when dealing with child welfare are: 1) written consent authorization 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.

### **Implementation: How**

As noted above, none of these three methods is required if the information and entities are covered by law such as 42 USC 671(a)(8) authorizing information sharing. Having said that, however, the three methods that can be employed are:

#### **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 parent.

#### **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 as 45 CFR 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.

#### **State Statute**

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.

Appendix A, Matrix One of this Toolkit entitled "Child Welfare" serves as additional guidance around sharing child welfare information.

The Children's Bureau Child Welfare Policy Manual (CWPM) provides departmental policies on CAPTA and titles IV-E and IV-B of the Act. The text of each law, including provisions on confidentiality and information sharing may be accessed on Children's Bureau website:

<http://www.acf.hhs.gov/programs/cb/laws-policies/federal-laws/laws>. The CWPM may be accessed at:  
<http://www.acf.hhs.gov/programs/cb/laws-policies/index.htm>.

### **Major Federal Laws and Regulations**

CAPTA; Child and Family Services Improvement and Innovation Act; Fostering

Connections to Success and Increasing Adoptions Act; title IV-B (Child Welfare Services and Promoting Safe and Stable Families), title IV-E (Federal Payments for Foster Care and Adoption Assistance), and, title XX (Block Grants to States for Social Services) of the Act.

## 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"). 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 but not limited to child support services, SNAP, employment assistance, child protective services and child welfare, Medicaid, and Unemployment Insurance.

States have broad flexibility to implement programs that best serve their distinct communities. 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 by that law.

Aside from a limited number of statutory requirements, states largely determine how the state TANF program shares information with other federally-funded programs, provided it is in accordance with applicable federal and state requirements, including the Privacy Act of 1974. State TANF programs may collaborate with other state programs to determine the information to be shared, the

legitimate governmental purpose for sharing, with whom and when to share the information and the mechanism for protecting the information once shared.

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), a system that allows the state TANF agency to exchange eligibility and benefit verification information with certain other databases, including state wage data, unemployment compensation benefits information, information maintained by the Social Security Administration, and unearned income information from the Internal Revenue Service. At the same time, it must take reasonable steps to restrict the use and disclosure of information about individuals and families applying for and/or receiving TANF benefits. The TANF statute imposes penalties on states that fail to participate in IEVS.

Furthermore, the requirement at sections 408(a)(2) and 408(a)(3) of the Social Security Act, and the regulations at 45 CFR 264.30, necessitate data sharing between TANF agencies and the child support enforcement agency. These provisions require TANF agencies to reduce cash assistance that would otherwise be available (and may eliminate it) if the child support enforcement agency determines that an

(TANF)

individual is not cooperating in establishing paternity, and 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) s/he 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 IV-D requirements.

Other areas where data sharing is necessary in order to comply with statutory requirements are to provide law enforcement with the current address of any cash assistance recipient (section 408(a)(9)(B) of the Social Security Act), and to collect, on a monthly basis, disaggregated case record information for families receiving SSI benefits, subsidized housing, Medicaid assistance, SNAP, or subsidized child care (section 411(a) of the Social Security Act). Federal statute or regulation does not dictate the method of data sharing; thus, it is up to state discretion, in accordance with applicable laws.

## Applicable Federal Legislation

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

States and tribes use their TANF funds to provide monthly cash assistance payments to low-income families with children, as well as a wide range of services that are “reasonably calculated” to address the program’s four broad purposes. These purposes are: providing assistance so children can remain with their families; supporting job

## Temporary Assistance for Needy Families

preparation, work and marriage; reducing out-of-wedlock pregnancies; and encouraging two-parent family formation. ACF encourages TANF programs to work in partnership with other federal, state, and local systems in an effort 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.

In an effort to protect individual information while also providing efficient and coordinated services, states must make decisions, based on its 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.

### Implementation: What and Who

For successful implementation of data sharing, states should consider forming two working groups: a program group and a legal group. The state agency heads should also enter into a MOU outlining what information will be shared, with whom, and by what method. Such an MOU should consider program data needs as well as applicable state and/or federal laws.

### The Program Group

The policy and practice experts will determine **what** data information should be exchanged. After the group agrees on the limited data set, it should determine **who** has access to the data, reviewing job functions and considering whether staff need to receive all or just a subset of the shared data. For example, in some states, child care programs use much of the same application data as the TANF program. If the child care program so

(TANF)

chooses, it may use a TANF eligibility determination in its own eligibility process.

## **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) protect TANF case information from being shared with other government systems. After examining applicable laws, the group should provide suggested vehicles 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 TANF agency to share the recipient's information.

However, the TANF agency should consider making clear that the applicant's information may be shared 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.

Appendix A, Matrix Two of this Toolkit entitled "Temporary Assistance for Needy Families (TANF)" serves as additional guidance around sharing TANF information.

## **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 CFR Parts 260 – 287; 45 CFR §205.51 – §205.60.

# Chapter 4. Child Support

---

## The Case for Sharing

**U**nless otherwise specifically authorized in title IV-D of the Social Security Act (the federal child support statute), the personal information that the 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). The system requires strict security requirements. At the same time, the law provides interface requirements in its management system: for example, the state's plan for child support must include certain information sharing with TANF, Foster Care, Medicaid, and SNAP.

States are also 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. Such automated data systems must be used for information comparison activities that shall 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 is provided by other systems to the child support system, but most of these data exchanges are not reciprocal. It is important to note that the child support statute clearly states that the child support system shall have access 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 information gathered under the authority of section 666(c)(1)(D) is then safeguarded and maintained solely by the child support system and cannot be disclosed by the state child support program unless separately verified from other systems or methods (e.g., postal verification as an example). State child support agencies are required to certify that their systems incorporate rigorous data safeguards, subject to IRS audits.

The Office of Child Support Enforcement (OCSE) within the U.S. Department of Health and Human Services maintains the Federal Parent Locator Service (FPLS), which includes the National Directory of New Hires (NDNH) and the Federal Case Registry (FCR). OCSE enters into MOUs or Computer Matching Agreements (CMA) with each federal or state agency that is authorized to receive FPLS information, including data from the NDNH. Authorized data users are



*“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, Office of Child Support Enforcement, 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, published in the Summer 2009, page 1.*

primarily state child support agencies and those federal and state needs-based programs specified by statute. The MOU or CMA specifies the purposes for sharing information,

the legal authority, the permitted purposes, 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 is very specific regarding the sharing of information, 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, as follows:

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

Title IV-D of the Act, as well as the enabling regulations, establishes standards for state paternity establishment for children and establishment and enforcement of child support orders for children. The Act, and implementing regulations, specifies when information will be shared, and specifies the kinds of information that can be shared and for what purpose, with the following state systems and entities:

- Authorized courts
- Child welfare
- Medicaid
- CHIP
- TANF
- SNAP
- State attorneys

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

If permitted by law, for systems to share data, the system heads still should develop and agree on an MOU and/or CMA regarding compliance with federal law on the use of

*In 2006 and 2007, the federal Office of Child Support Enforcement, through a contract with the Center for Policy Research, brought together eight (8) different local jurisdictions from eight (8) different states, with representatives from the child support and child welfare systems, to work out how to handle multiple-agency families and why child support and child welfare must collaborate. The jurisdictions were from California, Massachusetts, Minnesota, New Jersey, Oklahoma, Oregon, Tennessee, and Wisconsin, and ranged from the smallest local jurisdictions of approximately 400,000 (Hampden County, Massachusetts, Camden County, New Jersey, and Clackamas County, Oregon) to the largest local jurisdiction of Los Angeles County, California. The meetings resulted in a number of jurisdictions leading the way on how these two child-serving systems can work together.*

data and the secure maintenance of data. The MOU or CMA will aid systems administrators in determining the information to be shared, the purpose, and the federal statutory basis for sharing, as well

as the security safeguards required to store and process sensitive information such as NDNH data. Appendix A, Matrix Three, of this Toolkit provides additional guidance for sharing child support information with other programs and agencies.

### **The Program Group**

The program group, consisting of policy and practice experts from the child support and the other state programs legally authorized to access child support data, must follow the requirements of the federal law and determine **what** information is necessary to share,

cognizant that the minimal disclosure of necessary information remains the rule. **Who** has access to the child support information is dependent on presenting permissible reasons for the information sharing process. Again, the access is based on the person's responsibilities or the job classification's responsibilities and should be limited to only those persons who need to know this information in order to perform their job responsibilities and limited to the information necessary to perform their program responsibilities and to further provide and improve the permissible services to the youth and/or family.

*As discussed previously in the Child Welfare chapter, the Office of Child Support Enforcement and Children's Bureau issued a joint Information Memorandum (IM) dated August 1, 2012 (IM-12-02) that discusses information that the state child support agency can provide to the state child welfare agency to carry out their program responsibilities. This recent IM follows the revised child support enforcement regulations issued in December 2010 regarding the State Parent Locator Service (SPLS) and the Federal Parent Locator Service (FPLS) that permit state child support agencies to share certain information about parents and relatives of a child involved in a child welfare case with state child welfare agencies.*

### **Implementation: How**

#### **The Legal Group**

Since the authority for sharing information is statutory, the issue of voluntary consent by

the individual is not applicable. Nor would a state court order be a proper mechanism to obtain information from the child support services agency if not permitted by federal law. Therefore, the lawyers for both the child support and the other agencies must work together, with the information technology and security personnel, to ensure that the information shared is permitted by both federal and any applicable state laws, that the purpose for the sharing is authorized, including that the data to be shared is the minimum necessary to accomplish the mission, and that the information is safeguarded and maintained in a confidential manner once shared.

Appendix A, Matrix Three, of this Toolkit entitled “Child Support” serves as additional guidance around sharing child support information. It is important to note that Matrix Three has a unique format and context in that the child support program has significantly greater statutory restrictions on data sharing and safeguarding, and the matrix reflects this difference from the other matrices herein in order to assure clarity and understanding.

### **Major Federal Laws and Regulations**

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

# Chapter 5. Child Care

---

## The Case for Sharing

**F**or the past 20 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 Program of 1990 as amended, also known as the Child Care and Development Fund (CCDF). In many states, the 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, 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.

But unlike some of the other specific federal human services laws and regulations discussed in this Toolkit, the issues of confidentiality and information sharing are absent in the federal laws and regulations creating and regulating child care. Except as regulated by The Privacy Act of 1974, as amended, states determine the rules and practices for the sharing of information.

## Applicable Federal Legislation

### Child Care and Development Block Grant

The goal of the Child Care and Development Block Grant law is helping parents to access safe, quality child care while employed or enrolled in training/education. Key components of the child care law and federal regulations include:

- Lead state child care agency coordinates the provision of child care services with other federal, state, and local child care and early childhood development programs;
- Lead child care agency gives priority to children of families with very low family income and children with special needs;
- State child care agency accumulates specific case-level individual recipient reports including sources of income (including TANF, SNAP, housing assistance, etc.) and other demographic information; and,
- Eligibility criteria and priorities may relate to other human services programs (e.g., TANF, child protective services).

The law and applicable regulations regarding the Child Care and Development Block Grant program do not discuss confidentiality and information sharing. The individual states decide how case information, eligibility information, and other types of case matching can be shared with other governmental units.

### Interagency Partnerships

*The Race to the Top - Early Learning Challenge is jointly administered by the Department of Education and ACF/HHS. These grants are helping states to strengthen core components of an integrated early childhood system including program standards, data systems, early learning standards and assessment, health promotion and family engagement. See: [www.acf.hhs.gov/programs/ecd/programs/race-to-the-top](http://www.acf.hhs.gov/programs/ecd/programs/race-to-the-top)*

*ACF awarded grants to support State Advisory Councils to lead the development or enhancement of a high-quality, comprehensive system of early childhood development and care that ensures statewide coordination and collaboration among the wide range of early childhood programs and services in the state. See: <http://www.acf.hhs.gov/programs/ecd/programs/state-advisory-councils>*

ACF has encouraged states to align CCDF eligibility policies with other programs serving low-income families. In particular, states may establish longer eligibility periods to align with other programs, such as Head Start, Early Head Start, Supplemental Nutrition Assistance Program (SNAP), Medicaid, and the Children’s Health Insurance Program (CHIP). 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

With the absence of information sharing direction being provided by the child care law and regulations, the state’s federal limitations are found in The Privacy Act of 1974, 5 USC §552a, as amended. In addition to any state laws regarding confidentiality and privacy, the state must abide by and apply the requirements of The Privacy Act. The Privacy Act generally only binds federal agencies, and is not applicable to state and local government agencies—with some exceptions, such as computer matching issues, and requirements related to the disclosure and protection of Social Security Numbers (SSNs).

The Privacy Act clearly states that matching of individual data between different governmental agencies is permitted with prior written consent of the individual to whom the information pertains (§552a(b)), or unless pursuant to a court order whereupon advance written consent is not required (§552a(b)(11)). It is important for the different agency heads to develop a process of sharing information that will lead to a written MOU including the details of 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.

The MOU is particularly important for states with child care and education systems linked, meaning that confidentiality and privacy requirements of the education system (i.e., FERPA) may apply. Similarly, some states integrate the Head Start and Pre-K programs with the child care system, or do joint funding of child care with Head Start and Pre-K programs, so again, FERPA and information sharing requirements from other disciplines may be a consideration. But by the agency leaders creating a program group and a legal

group, the answers to these questions can be reached.

### The Program Group

The staff members from the agencies wishing to share individual case information represent the areas of policy, practice, and operations. This group forms the Program Group and will determine **what** information is minimally necessary to share, and **who** will have access to the information because they have a “reason to know” based on the legitimate governmental purpose for the information sharing,

When determining data elements to be shared, it is important to note that the state child care agency collects considerable case level data. On a monthly basis, each state’s lead agency completes the ACF 801 form for each family receiving child care grant assistance. The ACF-801 case-level data are then reported either monthly or quarterly. Quarterly data are reported 60 days after the end of each quarter and monthly data are due 90 days after the report month. All lead agencies in the States, the District of Columbia, and the Territories (Puerto Rico, American Samoa, Guam, Northern Marianna Islands, and the US Virgin Islands) are responsible for collecting and reporting ACF-801 data. States submit their records electronically to the Office of Child Care Information System. Lead agencies may submit either full population or a monthly sample (approximately 200 families) of subsidized child care recipients for the ACF-801.

The ACF 801 form covers case level data, household information (e.g., family size used for eligibility purposes), income (including employment, TANF, SNAP, SSI, other federal programs and federally-assisted

programs), child specific information (including date of birth, race, and gender), and child care setting information (including data elements on the quality of care). As a result, when dealing with the child care system, the Program Group has rich and current data, and decisions must be made about the least amount of information to be shared and, based on legitimate governmental purpose and job classifications, and with whom the information will be shared.

### Implementation: How

#### The Legal Group

The first task for the legal group is deciding whether or not the child care individual case record information is confidential and protected under state laws and policies, and to ensure compliance with The Privacy Act with regard to SSNs. This group must also accumulate state child care and general state privacy laws to determine if there are additional state requirements that must be met to share case information between systems working with the same person. The group must examine each state law to determine how it encourages information sharing to improve outcomes for this population as well as additional specific requirements. For each of the requirements, the Legal Group must provide suggested vehicles for sharing the information and meeting the requirements.

Since child care information may be protected under state laws and policies, and SSNs must be handled in accordance with The Privacy Act, the information sharing option generally to consider is prior written consent authorization by the parent or guardian. An authorization to share information can be drafted so that the individual “opts in,” or affirmatively agrees 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 must consult with the Program Group to determine the best course of action to proceed.

Appendix A, Matrix Four, of this Toolkit entitled “Child Care” serves as additional guidance around sharing child care information with other social services programs and agencies within human services and elsewhere.

### **Major Federal Laws and Regulations**

Child Care and Development Block Grant, 42 USC §658; The Privacy Act of 1974, 5 USC §552, as amended.

# 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. Similar to child care, as the table included in this document indicates, the issues of confidentiality and information sharing are absent in the federal laws and federal law and regulations regarding LIHEAP. Except as regulated by The Privacy Act of 1974, as amended, states determine the rules and practices for sharing of information.

## Applicable Federal Legislation

### Home Energy Grants

Home energy grants are funded through a block grant to states in an effort 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;

- Grants are made to households in which at least one individual is receiving TANF, SNAP or SSI;
- Programs are required to coordinate activities with child welfare programs and SSI; and,
- For verification of income eligibility purposes, states may apply procedures and policies consistent with TANF.

Again, it must be understood that the law and applicable regulations regarding LIHEAP do not specifically discuss confidentiality and information sharing. Therefore, the individual states decide how case and eligibility information and case matching can be shared with other governmental units.

### Implementation: What and Who

The LIHEAP federal law and the implementing regulations do not address information sharing. Therefore, the state’s federal limitations are found in The Privacy Act of 1974, 5 USC §552a, as amended. This federal law applies to questions of privacy of individual case information when the enacting law is silent on the subject. In addition to any state laws regarding confidentiality and privacy, the state must abide by and apply the requirements of The Privacy Act in looking at what information is to be shared, with whom, and how.

As stated in the previous chapter, The Privacy Act states that matching of individual data between different governmental agencies is



permitted with prior written consent of the individual to whom the information pertains (§552a(b)), or unless pursuant to a court order whereupon advance written consent is not required (§552a(b)(11)). The heads of the different governmental agencies should agree on legitimate governmental purposes and develop a process of sharing information leading to an MOU that includes the details of information sharing (what, when, with whom, and how). Data must also be confidentially maintained once shared. The agency leaders creating a program group and a legal group will answer these questions.

### **The Program Group**

The policy, practice, and operations representatives from the agencies wishing to share individual case information will answer the questions of **what** information will be shared (being cognizant that the information must be the minimally necessary data elements), and **who** will have access to the information based on the “need to know” doctrine and for a legitimate governmental purpose.

## **Implementation: How**

### **The Legal Group**

The LIHEAP individual case record information is confidential and protected under The Privacy Act. Therefore, this group must accumulate the state’s general privacy laws to determine if there are additional state requirements that must be met to share case information between systems working with the same person. After an examination of each applicable state law, the legal group will determine how the state law encourages, or at least does not inhibit, information sharing as well as any other additional specific

## Low Income Home Energy Assistance Program

requirements. For each of the requirements, the legal group must provide suggested vehicles for sharing the information and meeting the requirements.

Similar to child care, the information sharing option under The Privacy Act generally most appropriate for LIHEAP applicants/recipients is prior written consent authorization by the individual applicant. An authorization to share information can be drafted so that the individual “opts in,” or affirmatively agrees to share the 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.

The Legal Group should review the authorizations currently being used by the systems to determine whether a single authorization, used by both systems, may be the appropriate vehicle to enable information sharing. If so, the group should draft and provide to agency heads such an authorization for review and distribution to internal government (including but not limited to the Program Group) and external partners and other interested parties for comment.

Appendix A, Matrix Five, of this Toolkit entitled “Low Income Home Energy Assistance Program” serves as additional guidance around sharing LIHEAP information with other programs.

## **Major Federal Laws and Regulations**

Home Energy Grants, 42 USC §8621.

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

---

### The Case for Sharing

Commonly referred to as the Food Stamps program, the Supplemental Nutrition Assistance Program (SNAP) actively safeguards the personally identifiable information provided by applicants for and recipients of SNAP benefits. It does not, however, present any barriers to information sharing with other state human services systems and specifically gives an exception to the safeguards with federal public assistance programs and federally-assisted state programs.

The federal regulations further clarify that the federally-assisted state programs must provide assistance to low-income individuals on a means-tested basis, making SNAP an important partner in the state's information sharing initiatives. Obviously, food and nutrition affects and impacts all health and human services. Food and nutrition is central and essential to all persons' lives and to the success of the provision of all services.

To facilitate working in concert with other systems, SNAP requires a joint application process with TANF to reduce the burden on households. The client must be able to apply selectively just for SNAP benefits and the application must be limited to the individual providing his/her name, address, and signature. That is all that the state can require for a person to apply for SNAP benefits and the completion of those three items constitute, as defined by the federal law, an application.

When additional information is provided and the application is completed, a receipt of SNAP benefits is retroactive to the date of the earliest submission.

The law specifically states that information obtained by SNAP agencies can be provided to persons directly connected with programs which are required to participate in the state income and eligibility verification system (IEVS) to the extent that the SNAP information is useful in establishing or

*The state's child welfare SACWIS wanted to access the Food Stamp Program's file information. The Food Stamp Program made clear that its regulations permit disclosure of file information to "federally-assisted state programs providing assistance on a means-tested basis to low income individuals." The Food Stamp Program determined that the state SACWIS/Child Welfare Programs qualify as "federally-assisted programs" and therefore disclosure of Food Stamp Program file information to SACWIS/Child Welfare staff may be permitted. The information obtained may not be further disclosed to any other individual or agency that is not directly associated with the administration of the Child Welfare Programs.*

verifying eligibility or benefit amounts under these other programs.

Even if information from SNAP is permitted to be shared with other federal assistance programs, including means-tested programs for low-income individuals and families, notice must be given to food stamp applicants that information may be provided to other health and human service systems and of its use by those health and human service systems.

## Applicable Federal Legislation

### **Food Stamp Act of 1964, as amended, now known as the Supplemental Nutrition Assistance Program (SNAP)**

The federal law's purpose is to promote the general welfare and to safeguard the health and well-being of low-income households by raising levels of nutrition and by providing a mechanism to increase the food purchasing power of the poor. It is to alleviate the hunger and malnutrition of low-income and poor households and, at the same time, increase the use of the available agricultural abundance and strengthen the agricultural economy. Key components of the SNAP law and federal regulations regarding information sharing include:

- State SNAP agency must execute data exchange agreement with other agencies, specifying information to be exchanged and procedures used for the exchange;
- Privacy statement required for all SNAP applications and recertifications that information will be verified through computer matching programs and that information may be disclosed to other: 1) federal assistance programs; 2) federally-

### Supplemental Nutrition Assistance Program

assisted state programs providing assistance on a means-tested basis to low-income individuals; and, 3) persons directly connected with the administration or enforcement of the provisions of SNAP or its regulations. This is consistent with section 11(e)(8)(A)(i) of the statute and section 272.1(c)(1)(i) of SNAP regulations;

- Privacy statement also must contain a statement that the collection of information, including SSN, of each household member is authorized by law and information will be used to determine eligibility through computer matching programs;
- As a condition to receive SNAP benefits, both custodial parent and non-custodial parent must cooperate with the child support services agency;
- The statutes also allows for SNAP obtaining current support information directly from the state agency in lieu of obtaining information from the household;
- Exception to safeguards to permit use or disclosure of information to persons directly connected with administration of SNAP, federal assistance programs, or federally-assisted state programs providing assistance on means-tested basis to low-income individuals;
- State SNAP agencies must provide information to child support and SSI programs;
- Use or disclosure of information obtained from the food stamp program includes persons directly connected with the administration or enforcement of the programs which are required to participate in the state IEVS to the extent the food stamp information is useful in establishing or verifying eligibility or benefit amounts under those programs. SNAP state

agencies may exchange with state agencies administering other programs in IEVS information about food stamp households' circumstances which may be of use in establishing or verifying eligibility or benefit amounts under the Food Stamp Program and those programs, such as TANF; and,

- The recently-enacted Agriculture Act of 2014 (Farm Bill) requires state SNAP agencies to match participant data with wage data maintained in the NDNH.<sup>5</sup>

SNAP agencies may exchange IEVS information with these agencies in other states when it is determined that the same objectives are to be met and these programs are TANF, SNAP, Medicaid, Unemployment Compensation, and any state program administered under titles I, X, XIV (adult categories), or VVI (SSI) of the SSA. SNAP state agencies verify SSNs by submitting to SSA for verification.

Thus, the SNAP federal statutory framework presents a balance of protecting the confidentiality of the information provided to SNAP for eligibility or recertification purposes with the necessity to provide the information to other federal assistance programs and federally-assisted state programs providing assistance on a means-tested basis to low-income persons.

### Implementation: What and Who

As matrix six at Appendix A indicates, both SNAP and the regulations implementing the law provide that the state agencies with which SNAP can share information obtained from food stamp applicants or recipient households must be other federal assistance programs, or federally-assisted state programs providing

assistance on a means-tested basis to low income individuals, or general assistance programs, or persons directly connected with the administration or enforcement of the provisions of SNAP or its regulations.








The law and regulations discuss the requirement that the state agencies must execute a data exchange agreement and that such an agreement must specify the information to be exchanged and the procedures which will be used to exchange such information. Therefore, as a first step, the agency heads should agree that the process will lead to an executed MOU including information to be shared, with whom, and by what method. The MOU should also clearly state the legitimate governmental interest for the information sharing process and the recognition and support to balance such interest with the interests of confidentiality and privacy. To accomplish these goals resulting in an MOU, the agency leaders must form two working groups: a program group of policy, practice and operations experts from the different agencies, and a legal group representing both agencies.

### The Program Group

The policy, practice, and operations group is charged with determining **what** information to share, with the mandate to share only what is absolutely necessary and nothing more. The next task for the program group is to determine **who** has access to the information. Taking into consideration the legitimate governmental interests as the foundation for the information sharing process, the person's responsibilities or the job classification's responsibilities, and limiting access to the shared information to only those persons who have a "need to know" this information in order to perform their job responsibilities and

<sup>5</sup> Enacted as [H.R. 2642](#), 113<sup>th</sup> Congress..

to further provide and improve services to the household members. The group’s list might look something like this:

-  Name of each household member
-  Address
-  Social Security Number
-  Source of financial resources
-  Support income/obligations
-  Name of employer
-  Address of employer

## Implementation: How

### The Legal Group

The Legal Group truly has many purposes to fulfill and tasks to accomplish to assist the state agency in its information sharing efforts. Under SNAP, the Legal Group must confirm that the partner agencies are permitted to receive SNAP data as a Federal Assistance program, a federally-assisted state program providing assistance on a means-tested basis to low income individuals, or persons directly connected with the administration or enforcement of the provisions of SNAP or its regulations, or a general assistance program. Then taking the product of the Program Group, the Legal Group will draft the necessary MOU between the agencies as to specific information to be shared. As part of the Legal Group, the information technology experts from the partner agencies must work to determine the procedures used to exchange and protect information in order to accomplish the legitimate governmental purpose.

As part of this group’s responsibilities, the agency’s legal experts must review all state laws that apply to information obtained by the SNAP program and the other agencies, as well as, 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 of the additional state law requirements, the Legal Group must provide suggested vehicles for sharing the information and meeting the requirements. Such additional requirements may call for further work by the Program Group and the information technology experts.

As part of its responsibilities, the Legal Group will review the required privacy statement, for all SNAP applications and recertifications, that information will be verified through computer matching programs and that information provided by the households may be disclosed to other Federal Assistance programs or federally-assisted state programs providing assistance on a means-tested basis to low-income individuals, or persons directly connected with the administration or enforcement of the provisions of SNAP or its regulations. To take additional steps to give notice to SNAP applicants, the Privacy Statement may be amended to specifically notify the applicant that SNAP shared individual household information with particular other state agencies and that such information sharing is permitted by both federal and state laws.

Appendix A, Matrix Six, of this Toolkit entitled “Supplemental Nutrition Assistance Program” provides additional guidance around sharing SNAP data with other social services programs within human services.

## Major Federal Laws and Regulations

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

# Chapter 8. Information Technology Support To Confidentiality

---

## The Case for Sharing

**C**onfidentiality is fundamentally about how we control information. It is about sharing the information we want to share with the people or organizations with whom we can and want to share it, while also choosing those people or organizations with which we neither can nor will share information. The proper use of information technology can not only greatly facilitate the sharing of information; it can also greatly enhance both the security and the confidentiality of information in electronic form over that of paper-based information.

Consider that when you share a paper-based file folder, you have no control over what document in that folder the person sees. Once the file folder leaves your hands, you have neither control over its contents nor the ability to protect it. The person you shared it with could alter the contents or share it with someone else not approved to see it. When one person has the folder, no one else can view the information in that folder at the same time. And the meaning of the information in the folder may be interpreted differently by the person. It may be in a language the person does not understand, or it may use terms with which he or she is unfamiliar.

Using information technology, there are 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 accessed through a common web-based portal that draws data from multiple sources. Whatever the means though, the one constant is that, when properly designed, implemented and managed, information technology can facilitate the sharing, protect the confidentiality, and enhance the understanding of information.

## Enabling Information Sharing

Information may be shared in a number of ways and for a number of reasons. First, information sharing may be expressly permitted (rather than prohibited) under federal or state laws. For example, SNAP spells out the conditions and circumstances under which information may be shared. Similarly, The Privacy Act of 1974, as amended, applying to TANF, child support, child care, and LIHEAP, specifies the conditions and circumstances under which information can be shared. These federal laws specify the minimum thresholds of compliance. States may add additional requirements that go above and beyond these federal laws.

In addition to permitting the sharing of information, these laws may specify the requirements for individual consent to the sharing of information. The sharing of information may be directed by court order. For example, for children in foster care, the court can order that the providers of court-ordered services provide information

regarding the provision and results of such services.

Information technology can greatly enable information sharing in each of these situations. First, information systems are typically designed for a specific purpose and to address specific requirements. In other words, the most appropriate means to address the specific laws regarding sharing are usually built into the systems. This is particularly true of vendor supplied or commercial off-the-shelf software (COTS) where the requirements are typically built into the technical safeguards and controls of the software. For example, a case management system will normally restrict a caseworker's access to only that information that is relevant to his or her assigned cases.

Second, information technology systems can electronically record information relative to an individual's consent to share his or her information. A system can record an individual's positive or negative consent to share 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.

Finally, 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 of the most obvious advantages of sharing data electronically is that, unlike the

paper file folder, electronic information can be viewed by more than one person at a time. Although it cannot be updated by more than one person simultaneously, when updates are made, those changes would be viewable as well. In most cases, this all happens in the background and is managed by the software that manages the data.

Most modern information technology environments provide a means for sharing information directly between two or more connected systems. 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. When a child in foster care is returned to the custody of his mother, the child welfare system could automatically send a change in custody to the TANF office so that the child's benefits can immediately begin.



Alternatively, a public child welfare agency could provide specific access (limited as defined by the child welfare system), and vice versa, to a private provider of foster care services under contract with the public agency so that immediate and accurate information is

shared between the two agencies, both 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 central information technology facility where multiple 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.

### Enabling Confidential Sharing

While this Toolkit does not examine the requirements of confidentiality and security for health information under the Health Information Portability and Accessibility Act (HIPAA), the HIPAA Security Rule (45 CFR Part 164) is instrumental to understand in that its principles and guidelines are applicable to the sharing of any type of information where confidentiality is of utmost importance. The rules set forth both required and addressed standards related to administrative, physical, and technical safeguards. This chapter primarily addresses the technical safeguards (45 CFR §164.312).

In Alameda County, California, an enterprise-based reporting model called Social Services Integrated Reporting System (SSIRS) breaks down silos by moving legacy systems into a "container" that enables real time sharing of information for five major county departments: economic benefits (TANF), children and family services (child welfare, adoptions, juvenile probation, child care), adult and aging, employment services (welfare to work), and county administration and finance. Through MOUs between the

programs, court, education and health care, SSIRS provides a "single point of enrollment" and enables the agencies to see the "whole client."

### Access Control

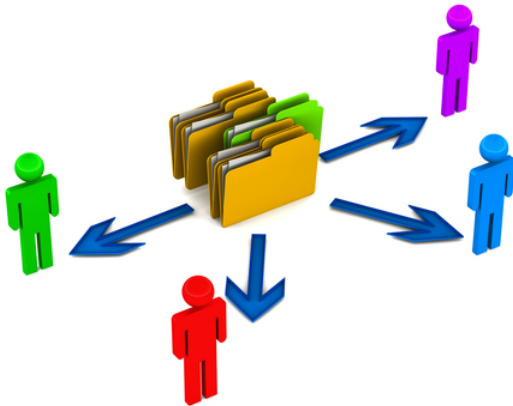
The first technical safeguard is access control (45 CFR §164.312(a)). Access control refers to the technical means used to control who can access an information technology resource. The simplest form of access control involves logging onto a computer system with a user ID and password. The user ID assigned to an individual is unique to that person and is typically only assigned after the person have verified his or her identity to the company, typically the employer, that is issuing the user ID. Therefore, the combination of the user ID and password is used to authenticate the person, (i.e., verify that they are whom they say they are) and to control access to the resources the person is allowed to access.

Unfortunately, the situation becomes a bit more complicated when more than one organization is involved. Each organization must protect its information, but each must also facilitate the sharing of that information through the use of information technology. Thus, true access control for a multi-organizational enterprise requires more robust authentication, authorization, and access control. It should determine what resources are authorized to be accessed by a user or process and prevent resources from being accessed by unauthorized users. This can be accomplished through the use of federated single sign-on (SSO) authentication capabilities which can address the cumbersome situation of logging on multiple times to access different resources or systems.



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 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.



Use of federated SSO begins with the creation of a federation. A federation is a group of two or more trusted partners with business and technical agreements that allow a user from one federated partner (participating agency, or organization) 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 granted access to the resources of another.

A well-defined set of attributes about users is securely exchanged between the two organizations. 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 by whom.

### **Audit Control**

Another technical safeguard called out in the Security Rule is audit control. Simply stated, the audit control requires that organizations implement a means to recording activity in the information system that involves use of electronic protected health information (45 CFR §164.312(b)). If we extend this concept beyond strictly protected health information, we find that the safeguard is applicable to other types of information as well.

Returning again to the example of sharing a paper file folder with another person, you may or may not record the fact that you shared the folder with a certain person on a particular date. Beyond that, you are unlikely to have any record if the folder is shared with someone else by the person with whom you shared it.

When properly implemented, the audit control will automatically keep an electronic record of everyone who creates, reads, updates or deletes any bit of 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 could be used to signal unauthorized attempts to access the information.

### **Integrity and Transmission Security**

The integrity (45 CFR §164.312(c)) and transmission security (45 CFR §164.312(e)) technical safeguards are related to one another in that a secure transmission also protects the integrity of the data. Also, both are intended to prevent an unauthorized party from reading or modifying information.

The integrity of information means that it has not been changed or altered in any unauthorized way. Such alterations could happen through intentional means, for example, when an individual with malicious intent tries to destroy or falsify information. It could also be through unintentional mean, 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.

Transmission security, on the other hand, 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.

*Building on New York City’s Mayor Michael Bloomberg’s strategy of “One City/One Community,” and very aware of the inefficiencies of government and the redundant activities for both citizens and city staff, the government created HHS-Connect, an interoperable plan to establish a client-centric approach to the service delivery systems in the city, 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. The organizations involved in this enterprise are the Administration for Children’s Services, Department for the Aging, Department of Correction, Department of Health and Mental Hygiene, Department of Homeless Services, Department of Juvenile Justice, Department of Probation, the Health and Hospitals Corporation, and the Human Resources Administration*

*For more information, or to read the actual Data Exchange Agreement and Executive Order that created HHS-CONNECT, follow this link:  
[http://www.nyc.gov/html/acs/download/pdf/mou\\_Inter\\_Agency\\_Data\\_Exchange\\_HHS\\_Connect.pdf](http://www.nyc.gov/html/acs/download/pdf/mou_Inter_Agency_Data_Exchange_HHS_Connect.pdf)*

Consider again the example of sharing a paper file folder with another person. If you send the folder through the mail, you have no guarantee that it reached its destination unaltered. Someone could have opened the envelope and changed the contents along the way. The mail carrier may have left the

envelope in the rain and the ink could have run and ruined the pages. When the other person is reading the files, you have no guarantee that someone else is not reading over his or her shoulder. Fortunately, a number of industry-standard security techniques can be implemented to ensure both integrity and transmission security.

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. 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.

Encryption also plays a role in transmission security. Secure transmission protocols are a part of most modern network infrastructures. These protocols 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.

### Enabling Shared Understanding

It is common for different organizations to use different terms to mean the same thing. One organization may refer to a person as a client, for example, while another refers to a person as a patient. For information sharing to work, these differences must be reconciled.

Semantics concerns the study of meanings. 'Semantic interoperability' is defined by the National Alliance for Health Information

Technology (NAHIT) as “the ability of different information technology systems, software applications and networks to communicate and exchange data accurately, effectively and consistently so providers can use the information as they care for patients.”<sup>6</sup> However, beyond the technical exchange of data, semantic interoperability implies that the meaning of data can be comprehended unambiguously by all parties in the exchange, and that information can be processed in a meaningful way.

One of the primary means of achieving semantic interoperability is through the use of data standards. Data standards provide agreed upon vocabulary and formats for exchanging, such as HL7, in the health care domain, and the National Information Exchange Model (NIEM) Human Services Domain which the Administration for Children and Families has established and manages on behalf of the Department of Health and Human Services.

Established in the Spring of 2012, the human services domain will be publishing numerous guidance documents addressing Information Exchange Package Documentation (IEPD – the term for a defined exchange standard for a specific dataset), including applicable process documents, procedural guides, training materials, and harmonization documents for synchronizing data across IEPDs. These tools and guidance are available at:

<https://www.niem.gov/communities/hs/Pages/about-hs.aspx>

Additional information on NIEM and the human services domain can be found at:

<http://www.acf.hhs.gov/initiatives-priorities/interoperability>.

---

<sup>6</sup> (<http://www.nahit.org>)

## Conclusion

Today we are at a crossroad in whether the next generation of health and human services systems will be more or less interoperable. States face tough economic times and the design and development of new automated public assistance, eligibility and related systems in the human services arena is viewed by many as cost prohibitive. For states that must seek alternatives to the costs of wholesale systems replacement, improved integration and data sharing across their existing, legacy systems is the next best option.

This Confidentiality Toolkit was written with all states in mind. Whether states design new systems from the ground-up, as some will do under the opportunities offered by the Affordable Care Act, or retrofit legacy systems with new, expanded electronic interfaces for enhanced data exchange, this Toolkit can help both. New systems development efforts will be able to “cook-in” data exchange standards and information sharing as foundational to the design. Legacy systems will also be able to use the Toolkit to reimagine data sharing across programs. Electronic data exchange interfaces will be rewritten and updated, replacing old, obsolete interfaces. Whether new systems replacement or legacy systems redesign, both types of project will benefit from this Toolkit.

Data sharing, and the protection of the privacy and confidentiality of the data being shared are, as we hope this Toolkit has shown, not mutually exclusive. Rather, with strong executive leadership driving the need to find a path forward, and with a collaborative approach between states’ program, policy and legal teams, the appropriate, timely sharing of data can ensure the privacy and confidentiality of client information while

simultaneously help our programs to improve service delivery, and ultimately, improve outcomes for our most vulnerable populations.

# Appendix A – Matrices

**DISCLAIMER:** This Toolkit is not intended to be relied upon as 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.

## Matrix One. Child Welfare

Title IV-B and IV-E of the Social Security Act-42 USC §621 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
629h(b)(1)(A)		Requires collaboration between courts and child welfare agencies to jointly plan for the collection and sharing of all relevant data and information.		
629m		Provides information regarding data standardization for improved data matching.		
671(a)(4)	State plan must assure coordination between programs at the State and local levels with federal programs, such as TANF, title IV-B programs, and Medicaid.			

Appendix A. Matrix One – Child Welfare

Title IV-B of the Social Security Act-42 USC §621 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
671(a)(8)		State plan must provide safeguards to restrict use or disclosure of information concerning individuals for purposes directly connected with administration of state’s plan approved under title IV-B and IV-E or other federal programs such as TANF, Child Support, Medicaid & SSI, as well as administration of any other federal or federally-assisted program which provides assistance (in cash or in kind) or services, directly to individuals on basis of need.		

Child Abuse Prevention and Treatment-42 USC §5101 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
5104(c)(1)(B)			Discusses consulting with the head of each agency involved with child abuse and neglect and the mechanisms for sharing information among other federal agencies for case management of clearinghouse.	
5106a(b)(2)(B)(viii)		State must have methods to preserve the confidentiality of all records to protect the rights of child and parents/guardians.		

Appendix A. Matrix One – Child Welfare

<b>Child Abuse Prevention and Treatment-42 USC §5101 et seq.</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
5106a(b)(2)(B)(ix)		State must disclose confidential information to any federal, state or local government entity, or any agency of such entity, that has a need for such information to carry out its responsibilities under law to protect children from child abuse and neglect.		

<b>Requirements Applicable to Titles IV-E and IV-B, 45 CFR §1355.50 et seq.</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
1355.53(b)(8)		Child welfare automated information system must ensure confidentiality and security of information and system.		

Appendix A. Matrix One – Child Welfare

<b>Requirements Applicable to Administration on Children, Youth and Families, Foster Care Maintenance Payments, Adoption Assistance, and Child and Family Services for Safeguarding information for the Financial Assistance Programs-45 CFR §205.50</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
205.50(a)	State plan for title IV-B and title IV-E funded programs and must include the following requirements.			
205.50(a)(1)(i)		Pursuant to state statute, imposing legal sanctions, the use or disclosure of information concerning applicants and recipients is limited to the purposes directly connected with one or more of the following:		
205.50(a)(1)(i)(A)	Administration of approved state plan under title IV-A, or state plan or program under titles IV-B, IV-D, IV-E, or IV-F or under titles I, X, XIV, XVI, XIX, or the SSI program established by title XVI. Such purposes include establishing eligibility, determining the amount of assistance, and providing services for applicants and recipients.			



Appendix A. Matrix One – Child Welfare

<b>Requirements Applicable to Administration on Children, Youth and Families, Foster Care Maintenance Payments, Adoption Assistance, and Child and Family Services for Safeguarding information for the Financial Assistance Programs-45 CFR §205.50</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
205.50(a)(1)(i)(C)	The administration of any other federal or federally-assisted program which provides assistance, in cash or in kind, or services, directly to individuals on the basis of need.			
205.50(a)(1)(i)(G)	The reporting to the appropriate agency or official of information on known or suspected instances of physical or mental injury, sexual abuse or exploitation, or negligent treatment or maltreatment of a child receiving aid under circumstances which indicate that the child’s health or welfare is threatened.			
205.50(a)(2)(i)	In the state plan, agency will have clearly defined criteria governing types of information that are safeguarded and conditions under where such information may be released or used. Types of information to be safeguarded include but are not limited to:			

Appendix A. Matrix One – Child Welfare

<b>Requirements Applicable to Administration on Children, Youth and Families, Foster Care Maintenance Payments, Adoption Assistance, and Child and Family Services for Safeguarding information for the Financial Assistance Programs-45 CFR §205.50</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
205.50(a)(2)(i)(A)	Names and address of applicants or recipients and amounts of assistance provided.			
205.50(a)(2)(i)(B)	Information related to social and economic conditions or circumstances of particular individual including information obtained from any agency pursuant to 205.55 (requesting and furnishing eligibility and income information); information obtained from the IRS and SSA must be safeguarded in accordance with procedures set forth by those agencies.			
205.50(a)(2)(i)(C)	Agency evaluation of information about a particular individual.			

Appendix A. Matrix One – Child Welfare

<b>Requirements Applicable to Administration on Children, Youth and Families, Foster Care Maintenance Payments, Adoption Assistance, and Child and Family Services for Safeguarding information for the Financial Assistance Programs-45 CFR §205.50</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
205.50(a)(2)(i)(D)	Medical data, including diagnosis and past history of disease/disability, concerning a particular individual.			
205.50(a)(2)(ii)	Release or use of information concerning individuals is restricted to persons/agency representatives who are subject to standards of confidentiality which are comparable to those of agency administering title IV-E or title IV-E programs.			
205.50(a)(2)(iii)	Except in an emergency, family or individual is informed whenever possible of a request for information from an outside source, and permission is obtained to meet the request. In emergency situation when consent for release of information cannot be obtained, individual will be notified immediately.			

Appendix A. Matrix One – Child Welfare

Other Reference	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
<p>Children’s Bureau website under SACWIS Overview and 45 CFR 1355.53(a) and (b)(2).</p>		<p>“If a State elects to implement a SACWIS, the system is expected to be a comprehensive automated case management tool that meets the needs of all staff.... By law, a SACWIS is required to support the reporting of data to the Adoption and Foster Care Analysis System (AFCARS) and the National Child Abuse and Neglect Data System (NCANDS). Furthermore, a SACWIS is expected to have bi-directional interfaces with a State’s title IV-A (Temporary Assistance for Needy Families), title XIX (Medicaid), and title IV-D (Child Support) systems.”</p>		

# Matrix Two. Temporary Assistance for Needy Families

Temporary Assistance for Needy Families-42 USC §601 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
602(a)(1)(A)(iv)		State TANF plan must outline how the State will take reasonable steps as state deems necessary to restrict use and disclosure of information about individuals and families receiving assistance under the program attributable to funds provided by the Federal government.		
608(a)(2)		State TANF agencies must reduce assistance that would otherwise be available (and may eliminate it) if the IV-D agency determines that an individual is not cooperating in establishing paternity or obtaining support (and there is no good cause exception).		

Appendix A. Matrix Two – Temporary Assistance for Needy Families

<b>Temporary Assistance for Needy Families-42 USC §601 et seq.</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
608(a)(9)(B)		Exchange of recipient’s current address information permitted with law enforcement agencies if officer furnishes agency with the name of the recipient and notifies the agency that individual falls under section 409 (a)(9)(A) or the individual has information that is necessary for law enforcement to conduct official duties and the location or apprehension is within such official duties.		
611(a)(1)(A)		States collect, on a monthly basis, disaggregated case record information for families receiving SSI benefits, subsidized housing, Medicaid assistance, SNAP, or subsidized child care.		

Appendix A. Matrix Two – Temporary Assistance for Needy Families

Grants to States for Public Assistance Programs-45 CFR §205 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
<p><b>205.51 – 205.60 (incorporated in TANF via 264.10). See also section 1137 of the Social Security Act.</b></p>		<p>Implements section 1137 of the Social Security Act. Please see individual provisions for specifics.</p>		
<p><b>264.30; section 408(a)(2) and (a)(3) of the Social Security Act</b></p>		<p>State must refer individuals to child support services for children for whom paternity has not been established or a support order needs to be established, modified or enforced.</p> <p>Child support IV-D agency must advise TANF agency if individual is not cooperating (unless individual qualifies for an exception under Federal law).</p> <p>TANF state agency must then reduce the TANF assistance (or could deny TANF assistance at State option).</p>		

# Matrix Three. Child Support

- 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 CP or child.
- See Section 453(b)(2) of the Act for the release process for the court or agent of the court.

LOCATING PARENTS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)				
Authorized Person/Program	Authorized Purpose of the Request	Persons About Whom Info May Be Asked	Sources Searched	Authorized Information Returned
Agent/attorney of a State who has the duty or authority to collect child and spousal support under the IV-D plan. Tribal IV-D having in effect an intergovernmental agreement with a State IV-D agency, for the provision of Federal PLS services.  <b>Section 453(c)(1) and 454(7)</b>	Agent/attorney of a State who has the duty or authority to collect child and spousal support under the IV-D plan. Tribal IV-D having in effect an intergovernmental agreement with a State IV-D agency, for the provision of Federal PLS services.  <b>Section 453(c)(1) and 454(7)</b>	Agent/attorney of a State who has the duty or authority to collect child and spousal support under the IV-D plan. Tribal IV-D having in effect an intergovernmental agreement with a State IV-D agency, for the provision of Federal PLS services.  <b>Section 453(c)(1) and 454(7)</b>	Agent/attorney of a State who has the duty or authority to collect child and spousal support under the IV-D plan. Tribal IV-D having in effect an intergovernmental agreement with a State IV-D agency, for the provision of Federal PLS services.  <b>Section 453(c)(1) and 454(7)</b>	Agent/attorney of a State who has the duty or authority to collect child and spousal support under the IV-D plan. Tribal IV-D having in effect an intergovernmental agreement with a State IV-D agency, for the provision of Federal PLS services.  <b>Section 453(c)(1) and 454(7)</b>



Appendix A. Matrix Three – Child Support

<b>LOCATING PARENTS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</b>
<p>Court that has the authority to issue an order against an NCP for the support and maintenance of child, or to serve as the initiating court in an action to seek a child support order.</p> <p><b>Section 453(c)(2)</b></p>	<p>To facilitate the location of any individual who is under an obligation to pay child support, against whom such an obligation is sought, or to whom such an obligation is owed. Locate a parent or child involved in a non-IV-D child support case.</p>	<p>Noncustodial Parent Custodial Parent Putative Father Child</p> <p><b>Section 453(a)(2)(A)</b></p>	<p>Federal Parent Locator Service In-state sources in accordance with State law</p>	<p><b>The Six Elements:</b> Person’s Name Person’s SSN Person’s address Employer’s name Employer’s address Employer ID Number</p> <p><b>Section 453(a)(2)(A)(iii)</b></p> <p>Wages, income, and benefits of employment, including health care coverage</p> <p><b>Section 453(a)(2)(B)</b></p> <p>Type, status, location, and amount of assets of, or debts owed by or to the individual</p> <p><b>Section 453(a)(2)(C)</b></p>

Appendix A. Matrix Three – Child Support

<b>LOCATING PARENTS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</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>	To facilitate the location of any individual who is under an obligation to pay child support, against whom such an obligation is sought, or to whom such an <b>obligation is owed, or who has or may have parental rights with respect to the child.</b> Locate a parent or child involved in a non-IV-D child support case.	Noncustodial Parent Putative Father	Federal Parent Locator Service. In-state sources in accordance with State law	<b>The Six Elements</b> , plus 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>
State agency that is administering a Child and Family Services program (IV-B) or a Foster Care case and Adoption IV-E program. <b>Sections 453(c)(4), 453(j)(3) and 454(8)</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)(A)(iv)</b>	Noncustodial Parent Putative Father Custodial Parent Child <b>Sections 453(a)(2)(A), 453(j)(3), and 454(8)</b>	Federal Parent Locator Service In-state sources in accordance with State law	<b>The Six Elements:</b> 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>  Wages, income, and benefits of employment, including health care coverage  Type, status, location, and amount of assets to, or debts owed by or to the individual <b>Section 453(a)(2)(B) and (C)</b>

Appendix A. Matrix Three – Child Support

<b>LOCATING PARENTS THROUGH THE STATE PARENT LOCATOR SERVICE (SPLS)</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info 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>Sections 453(c)(4), 453(j)(3) and 454(8)</b>	To assist states in carrying out their responsibilities under title IV-B and IV-E programs. <b>Sections 453(j)(3) and 454(8)</b>	Relatives of a child involved in a IV-B or IV-E case.	Federal Parent Locator Service In-state sources in accordance with State law.	<b>The Six Elements:</b> 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>

<b>AUTHORITY FOR STATE IV-D AGENCIES TO RELEASE INFORMATION TO NON-IV-D FEDERAL, STATE AND TRIBAL IV-D PROGRAMS</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</b>
<b>Sections 453A(h)(2) and 1137 of the Act</b> – State Directory of New Hires	Income and eligibility verification purposes of designated programs.	State agencies administering title IV-A, Medicaid, unemployment compensation, SNAP, or other State programs under a plan approved under title I, X, XIV, or XVI of the Act.	SDNH information: Individual’s name, address and SSN; employer’s name, address, and Federal employer identification number	

Appendix A. Matrix Three – Child Support

<b>AUTHORITY FOR STATE IV-D AGENCIES TO RELEASE INFORMATION TO NON-IV-D FEDERAL, STATE AND TRIBAL IV-D PROGRAMS</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</b>
<p><b>Sections 453 and 454A(f)(3) of the Act, Section 1102 of the Act; and 45 CFR 307.13.</b></p>	<p>To perform State or Tribal agency responsibilities of designated programs.</p>	<p>State or Tribal agencies administering title IV, XIX, and XXI, and SNAP programs.</p>	<p>Confidential information found in automated system</p>	<p>No Internal Revenue Service information unless independently verified.</p> <p>No MSFIDM or State FIDM information provided.</p> <p>No NDNH and FCR information for title XIX and XXI unless independently verified.</p> <p>For IV-B/IV-E, for purpose of section 453(a)(2) of the Act can have NDNH and FCR information without independent verification.</p> <p>-Any other purpose requires independent verification.</p> <p>For IV-A NDNH/FRC information for purposes of section 453(j)(3) of the Act without independent verification.</p> <p>-Need verification for other purposes.</p>

Appendix A. Matrix Three – Child Support

<b>AUTHORITY FOR STATE IV-D AGENCIES TO RELEASE INFORMATION TO NON-IV-D FEDERAL, STATE AND TRIBAL IV-D PROGRAMS</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</b>
<b>Sections 453A(h)(2) and 1137 of the Act</b> – State Directory of New Hires	Income and eligibility verification purposes of designated programs.	State agencies administering title IV-A, Medicaid, unemployment compensation, SNAP, or other State programs under a plan approved under title I, X, XIV, or XVI of the Act.	SDNH information: Individual’s name, address and SSN; employer’s name, address, and Federal employer identification number	

<b>LOCATING AN INDIVIDUAL SOUGHT IN A CHILD CUSTODY/VISITATION CASE</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</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 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>

Appendix A. Matrix Three – Child Support

<b>LOCATING AN INDIVIDUAL SOUGHT IN A PARENTAL KIDNAPPING CASE</b>				
<b>Authorized Person/Program</b>	<b>Authorized Purpose of the Request</b>	<b>Persons About Whom Info May Be Asked</b>	<b>Sources Searched</b>	<b>Authorized Information Returned</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. 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>

# Matrix Four. Child Care

Child Care and Development Block Grant-42 USC §658	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
658A(b)(4)	One goal is assisting parents to achieve independence from public assistance.			
658D(b)(1)(D)	Lead agency coordinates provision of child care services with other federal, state and local child care and early childhood development programs.			
658E(c)(2)(H)	State must demonstrate how it will meet the specific child care needs of families receiving or at risk of receiving TANF and who, through work activities, will transition from TANF.			
658K(a)(1)(v)	On a monthly basis, state must collect information regarding sources of family income including TANF, housing, or SNAP assistance.			

Child Care and Development Fund-45 CFR §§98 and 99 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
98.1(4)	Goal is to assist parents to achieve independence from public assistance.			

Appendix A. Matrix Four – Child Care

<b>Child Care and Development Fund-45 CFR §§98 and 99 et seq.</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
98.14(a)(1)(A) & (D)	In developing state plan, agency must coordinate child care services with other federal, state and local childhood development programs, public health agencies, public education, and TANF.			
98.20	Provisions for child’s eligibility for child care services and how eligibility requirements interface with other federal programs (i.e. TANF, child welfare).			
98.33(b)	State agency informs parents receiving TANF about work conditions and that exception to work condition is requirement to demonstrate inability to obtain needed child care for child(ren) under age six.			
98.44	Lead agency shall give priority for services to children of families with very low family income and children with special needs.			
98.71(a)(6)	Lead agency submits quarterly case-level report to HHS which includes sources of family income (TANF, housing assistance, SNAP, other).			
98.71(a)(13)	In these reports, the head of the household’s SSN is included if provided.			



Appendix A. Matrix Four – Child Care

<b>Guidance &amp; Other References</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
ACF 801 Form and instructions	Format for the case-level information collected on a monthly basis by state child care agency and reported to HHS on a quarterly basis.			
ACYF-PI-CC-00-04	Program instructions issued by Child Care Office regarding collection of SSNs in the eligibility process.			

## Matrix Five. Low Income Home Energy Assistance Program (LIHEAP)

Home Energy Grants-42 USC §8621 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
8622(1)(E)	Included in the definition of “emergency” is a significant increase in participation in a public benefit program including SNAP, SSI, and TANF.			
8624(b)(2)(A)	Home energy grants are made to households in which one or more individuals are receiving TANF, SSI, and SNAP.			
8624(b)(4)	LIHEAP must coordinate its activities with similar and related programs including those administered under title IV-B, title XX, and SSI.			
8624(i)	Certain recipients receiving SSI are not categorically eligible to receive energy assistance grants based solely on their status as SSI recipients.			
8624(j)	To verify income eligibility, state may apply procedures and policies consistent with TANF.			

## Matrix Six. Supplemental Nutrition Assistance Program (SNAP)

Supplemental Nutrition Assistance Program- 7 USC §§2011 et seq.	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
2014(a)	Categorically eligible if receives TANF, SSI, or Aid to the Aged, Blind, or Disabled benefits.			Requires joint application of SNAP and TANF to reduce burden on household. Require that the client be able to pick just to apply for SNAP if that is what client wants to do. All must provide to submit SNAP application is name, address and signature, if additional required information is subsequently provided. That submission wouldn't receive benefits, but would count as application date for later receipt of benefits when additional information is provided.
2014(d)	Exclusions from household income may include cash assistance under TANF, medical assistance, old age and survivors benefit payments, and Supplemental Security Income (SSI).			

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

<b>Supplemental Nutrition Assistance Program- 7 USC §§2011 et seq.</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
<b>2014(g)(6)</b>	Exclusions of financial resources from title IV-A and medical assistance.			
<b>2014(n)</b>	Allows for obtaining current support information directly from state agency in lieu of obtaining information from household.			
<b>2015(c)(3)</b>	Reports by households can be filed at same time for SNAP and TANF.			
<b>2015(l)(1)</b>	Requires custodial parent cooperation with paternity/support.			
<b>2015(m)(1)</b>	Requires non-custodial parent cooperation with paternity/support.			
<b>2020(e)(8)</b>	Exception to prohibition on disclosure of household information, allowing use or disclosure of such information to persons directly connected with administration of SNAP, federal assistance programs, federally-assisted state programs, the Comptroller General, and federal and state law enforcement authorities.			

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
272.1(c)(1)		<p>Use or disclosure obtained from food stamp applicant/recipient households shall be restricted to:</p> <p>(i)Persons directly connected with administration or enforcement of Food Stamp Act or regulations, other federal assistance programs, federally-assisted state programs providing assistance on a means-tested basis to low income individuals, or general assistance programs</p> <p>(ii)Persons directly connected with administration or enforcement of programs which are required to participate in state IEVS to the extent the food stamp information is useful in establishing or verifying eligibility or benefit amount under those programs</p> <p>(iii)Persons directly connected with verification of immigration status of aliens applying for food stamp benefits, through Systemic Alien Verification for Entitlements (SAVE) Program to the extent information is necessary to identify individual for verification purposes</p> <p>(iv)Persons directly connected with the administration of the Child Support Program in order to assist in its administration,</p>		<p>Working through some of this with General Counsel now. If distributed through block grant, is it a federally-assisted state program?</p>

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
		<p>and establishing or verifying eligibility or benefits under titles II and XVI of the SSA</p> <p>(vi) Local, state, or federal law enforcement officials, upon written request (including identity of individual requesting information and authority to do so, violation being investigated, and identity of person on whom the information is requested), for purpose of investigating alleged violation of Food Stamp Act or regulation</p> <p>(vii) Local, state, or federal law enforcement officials, upon written request for purpose of obtaining address, social security number, and, if available, photograph of any household member, if member is fleeing to avoid prosecution or custody</p> <p>(viii) Local educational agencies administering National School Lunch Program for purpose of directly certifying the eligibility of school-aged children for receipt of free meals under School Lunch and School Breakfast programs.</p>		

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
272.8(a)(1)		<p>State agencies may maintain and use an IEVS; state agencies may request wage and benefit information and use that information to verify eligibility for and amount of food stamp benefits due to eligible households; including any considered excluded household members and their SSNs. Information provider agencies include:</p> <ul style="list-style-type: none"> <li>(i) SWICA which maintains wage information</li> <li>(ii) SSA, including information available from SSA regarding federal retirement, and survivors, disability, SSI and related benefits</li> <li>(iii) IRS</li> <li>(iv) Agency administering UI Benefits.</li> </ul>		

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program	Unconditional Information Sharing	Conditional Information Sharing	Methods of Conditional Information Sharing	Comments and Suggestions
272.8(a)(2)		<p>State agencies may exchange with state agencies administering certain other programs in IEVS information about food stamp households' circumstances which may be of use in establishing or verifying eligibility or benefits amounts under Food Stamp Program and those programs. State agencies may exchange such information with these agencies in other states when they determine that same objectives are like to be met and these programs are:</p> <ul style="list-style-type: none"> <li>(i) TANF</li> <li>(ii) Medicaid</li> <li>(iii) Unemployment Compensation</li> <li>(iv) SNAP</li> <li>(v) Any state program administered under titles I, X, XIV (adult categories) or XVI (SSI) of SSA.</li> </ul>		
272.8(a)(3)		<p>State agencies must provide information to Child Support and titles II and XVI (SSI) of SSA.</p>		
272.8(a)(4)		<p>State agencies must execute data exchange agreement with other agencies, specifying information to be exchanged and procedures which will be used to exchange information.</p>		



Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

<b>Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
<b>273.2(b)(4)(i)</b>	Food Stamp application and recertification form must contain Privacy Act statement that the collection of information, including SSN of each household member is authorized by law and information will be used to determine eligibility or continuation of eligibility by comparing through computer matching programs.			
<b>273.2(b)(4)(ii)</b>		Application and recertification information may be disclosed to other federal and state agencies, including for law enforcement purposes.		
<b>273.2(b)(4)(iii)</b>		Should a claim arise against a household, application information, including SSNs, may be released to federal, state, and private agencies for claims collection.		
<b>273.2(b)(4)(iv)</b>		Food Stamp application may be denied if all application information, including SSNs, is not provided.		

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

<b>Food and Nutrition Service- 7 CFR Parts 271-285 Food Stamp Program</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
<b>273.2(f)(1)(i)-(xiv)</b>	State agencies required to verify following prior to certification by submitting to SSA for verification: gross nonexempt income; citizenship (if questionable) alien status; utility expenses; medical expenses; social security numbers; residency; identity; disability; food stamp eligibility factors; household composition; student status; child support; able body adults status for food stamp eligibility.			
<b>273.2(f)(7)</b>	SSI benefits verified by state agency through State Data Exchange (SDX) and social security benefits through Beneficiary Data Exchange.			
<b>273.2(k)(1)(iii)(A)(3) &amp; (D)</b>	State agency may verify SSI status through SDX and Beneficiary Data Exchange.			
<b>273.6(f)</b>	Access to information regarding applicants or participants who receive title XVI benefits using the SDX.			
<b>273.7(h)(4)</b>	If work related information provided by household is questionable, state agency must verify.			
<b>273.11(e)</b>	Residents of drug and alcohol treatment and rehabilitation programs are eligible for SNAP but must share application information to the treatment center and to the state agency.			

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

<b>Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
<b>273.11(j)(1)</b>	Regarding reduction of public assistance benefits, the state agency, rather than the household, shall be responsible for obtaining information regarding sanctions of individuals from other programs and changes in those sanctions.			
<b>273.11(k)</b>	If a disqualification is imposed on a member of a household for failure to perform an action required under means-tested public assistance program, state agency may impose same disqualification on member under SNAP.			
<b>273.11(l)</b>	Can sanction family where minor children fails to attend school or adult fails to work on attaining a secondary school diploma or recognized equivalent.			
<b>273.11(o)(1)</b>	State’s option to disqualify custodial parent for failure to cooperate with Child Support program.			
<b>273.11(p)(1)</b>	State’s option to disqualify non-custodial parent for failure to cooperate with Child Support program.			

Appendix A. Matrix Six – Supplemental Nutrition Assistance Program (SNAP)

<b>Food and Nutrition Service-7 CFR Parts 271-285 Food Stamp Program</b>	<b>Unconditional Information Sharing</b>	<b>Conditional Information Sharing</b>	<b>Methods of Conditional Information Sharing</b>	<b>Comments and Suggestions</b>
274.8(b)(10)(i)	State agencies are responsible to establish telecommunication links and any other arrangement with other state agencies necessary for interoperable transactions to such other state Electronics Benefit Transfer (EBT) authorization systems.			

# Appendix B - Memorandums of Agreement and Understanding, Security Agreements, and Notices of Privacy Practices

## State of Kentucky – Memorandum of Agreement

---

The following data sharing agreement is executed between Kentucky’s child support agency and the state’s Health Benefits Exchange. The agreement addresses the purposes, restrictions, roles and responsibilities, security, and other aspects of data protections relative to the request, use, and confidentiality and protection of data to and from the Kentucky Automated Support Enforcement System (KASES) and the Health Benefits Exchange (HBE) system, shared electronically by the two agencies on a routine basis.

### MEMORANDUM OF UNDERSTANDING

for the purposes of

#### DATA SHARING

Between

***Office of the Kentucky Health Benefit Exchange***

and

***Kentucky Department for Income Support***

***Child Support Enforcement***

This memorandum is entered into by and between the Office of the Kentucky Health Benefit Exchange (hereafter referred to as “the Office”) and Kentucky Department for Income Support, Child Support Enforcement (hereafter referred to as “Second Party”).

Whereas, the Parties shall exchange data that is confidential and must be afforded special treatment and protection; and,

Whereas, data exchanged by the Parties may be used or disclosed only in accordance with this memorandum and state and federal law;

Now, therefore, the Office and Second Party agree as follows:

1. **Purpose of Memorandum.** The purpose of this memorandum is to govern the exchange of Department of Public Health WIC Program Data for the Health Benefit Exchange program (alternatively referred to as the “American Health Benefit Exchange” or “Exchange”) which is further defined and explained in 45 CFR §155.100, 45 CFR §155.110, Governor’s Executive Order 2012-587, and Governor’s Executive Order 2012-783.
2. **Justification of Access.** This Memorandum is authorized by law under section 45 CFR §155.100, 45 CRR §155.110, Governor’s Executive Order 2012-587, and Governor’s Executive Order 2012-783.

45 CFR §155.100 allows each state to establish a health care benefits exchange that facilitates the purchase of health insurance.

45 CFR §155.110 authorizes exchanges established by a state to enter into agreements with eligible entities to carry out one or more responsibilities of the Exchange. Eligible entities are defined as entities that: (1) are Incorporated under, and subject to the laws of, one or more States; (2) have demonstrated experience on a State or regional basis in the individual and small group health insurance markets and in benefits coverage; and (3) are not a health insurance issuer or treated as a health insurance issuer under subsection (a) or (b) of section 52 of the Internal Revenue Service Code of 1986 as a member of the same controlled group of corporations as a health insurance issuer. Eligible entities also may include the State Medicaid agency, or any other State agency that meets the qualifications of 45 CRR §155.110(a)(1).

Governor’s Executive Order 2012-587 gives the Office the authority to enter into contracts and other agreements with appropriate entities, including but not limited to federal, state, and local agencies, as permitted under 45 CRR §155.110, to the extent necessary to carry out its duties and responsibilities, provided that such agreements incorporate adequate protections with respect to the confidentiality of any information to be shared.

KRS 205.712(2)(a) vests Child Support Enforcement with the authority to serve as the state agency to administer Part D of Title IV of the Social Security Act, 42 USC secs. 651 to 669;

Pursuant to the Social Security Act, 42 USC 654a, Kentucky must administer the child support program via a single statewide automated data processing and information retrieval system, such system being known as KASES;

This Memorandum implements the above referenced federal regulations and executive order by putting into place protections regarding the confidentiality of any information being shared between the parties.

3. **Description of Data:** Pursuant to the terms of this Memorandum, Second Party shall disclose the following data elements:

- **Non-custodial Parent Referrals**

KHBE → KASES	During the KHBE application process, if a client indicates a non-custodial relationship, then non-custodial information is gathered and a case referral is sent to KASES. KHBE case and member updates will be sent in this interface as well.	Daily
--------------	--	-------

- **Non-cooperation Data**

KASES → KHBE	KASES will send to KHBE client non-cooperation information as this can affect Medicaid eligibility.	Daily
--------------	---	-------

4. **Method of Data Transfer.** The data described in the Memorandum will be transferred via secure FTP site to the Office or its designee.
5. **Point of Contact.** For the purpose of this Memorandum, the Office designates as its point of contact for technical needs.

Holly Coffey  
 12 Millcreek Park  
 Frankfort, KY 40601  
 502-564-0105

For the purpose of this Memorandum, the Office designates as its point of contact for security purposes:

Name and Address

For the purpose of this Memorandum, the Second Party designates as its point of contact for technical needs.

Name and Address

For the purpose of this Memorandum, the Second Party designates as its point of contact for security purposes:

Name and Address

6. **Payment.** The Parties shall provide the data specified in this Memorandum at no cost.
7. **Permissible Uses and Disclosures of Data.** The Parties shall have on file with their respective Offices, a signed **Privacy and Security of Protected Health, Confidential and Sensitive Information** form for each person handling the specified Second Party data described in enumerated paragraph three (3) of this agreement. Both parties shall require all employees and contractors to sign confidentiality agreements annually.

The Office and the Second Party shall not use or further disclose, transmit, copy, or disseminate the data specified in the Memorandum except as in furtherance of the goals and purposes of the Health Benefit Exchange program, as defined and explained in the above-cited federal regulations and executive order, or as required by federal or state law.

The Office and the Second Party shall establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent unauthorized use or access to the data, specified in the Memorandum.

The Office and the Second Party shall not release or allow the release of the data specified in this Memorandum to any person or entities other than as permitted by this Memorandum.

The Office and the Second Party shall restrict disclosure of the data specified in this Memorandum to the minimum number of individuals who require the information in order to perform the functions of this Memorandum. The Parties shall instruct individuals to whom the data is disclosed of all obligations under this Memorandum.



The Office and the Second Party shall secure the data specified in this Memorandum when the data is not under the direct and immediate control of an authorized individual performing the functions of this Memorandum. The Parties shall notify each other by certified mail, return receipt requested, or in person with any proof of delivery within five (5) business days of discovery of any use or disclosure of the data not provided for by this Memorandum of which a party is aware.

A violation of this section shall constitute a material breach of this Memorandum.

8. **Disclosure to Agents.** The Office and the Second Party shall ensure that any agents, including, but not limited to, a contractor or subcontractor, to whom the Office and the Second Party provides the data specified in this Memorandum agree to the same terms, conditions, and restrictions that apply to the party with respect to the data.
9. **Access to Data.** Either party shall notify the other in writing, by certified mail, return receipt requested, or in person with proof of delivery within ten (10) days of any requests for access to data received from individuals who are not members of an organization with which the Office has a Memorandum of Understanding in place.
10. **Penalties.** The Parties acknowledge that failure to abide by the terms of this Memorandum may subject them to penalties for wrongful disclosure under applicable state and federal laws.
11. **Disposition of Data.** The Parties may retain the data specified in this Memorandum for the time required by the normal business processes of Child Support Enforcement, hereinafter referred to as the retention date. Upon the retention date, the Parties shall destroy all datasets and files. Protections under this Memorandum shall survive the termination of the relationship between the Parties, and the Parties shall protect the confidentiality of, and prevent unauthorized use or access to, the datasets retained.
12. **Terms of Memorandum.** This Memorandum shall be effective upon execution by both Parties and shall remain in effect until modified or cancelled by either Party. Any Party may initiate termination and cancellation of this Agreement upon written notice outlining the reasons for cancellation and allowing a ninety (90) day opportunity for the non-terminating Party to mitigate the breach and implement corrective procedures. If mitigation fails, the initiating Party will immediately issue a second written notice that cancellation will become effective thirty days from the date of the second notice. Notice of termination shall be delivered by certified mail, return receipt requested, or in person with proof of delivery.

The terms of this Memorandum may not be waived, altered, modified, or amended except by written Memorandum of both Parties.

This Memorandum supersedes any and all Memorandums by the Parties with respect to the use of data specified in this Memorandum. This Memorandum is binding upon, and inures to the benefit of, the parties and their respective successors and assigns. Changes in the individual members serving on the Advisory Board shall not be construed to in any way undermine the binding and enforceable nature of this Memorandum.

In witness whereof, the Office and Second Party have caused this Memorandum to be signed and delivered by their authorized representatives as of the date set forth below.

\_\_\_\_\_  
Signature  
**Name**  
**Executive Director**  
**Office of the Kentucky Health**  
**Benefit Exchange**

\_\_\_\_\_  
Signature  
**Name**  
**Commissioner**  
**Department for Income Support**  
**Child Support Enforcement**

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

## State of New York – Master Memorandum of Understanding

---

The following data sharing agreement is executed within the State of New York's human services department for and between various state public assistance programs and other agencies. The agreement addresses the data sharing roles and responsibilities, and other aspects of data protections relative to the request, use, and confidentiality and protection of program data received and shared with other state law enforcement, judicial, education, health, and human services agencies.

### AGREEMENT

#### Amendment

The data sharing agreement by and between the Department of Health and the Office of Children and Family Services is hereby amended to provide as follows.

AGREEMENT by and between the NEW YORK STATE OFFICE OF CHILDREN AND FAMILY SERVICES, 52 Washington Street, Rensselaer, New York (hereinafter called OCFS), and the NEW YORK STATE DEPARTMENT OF HEALTH, Corning Tower, Empire State Plaza, Albany New York (hereinafter called DOH).

WITNESSETH:

WHEREAS, OCFS, as the single State agency responsible for the implementation of the State Plan for the Foster Care maintenance Payments Program and the Adoption Assistance Program established pursuant to Title IV-E of the Social Security Act, is responsible for supervising the activities of social services districts and voluntary authorized agencies in the reception, care and placement of foster care and the administration of the adoption subsidy program; and

WHEREAS, OCFS, as the single State agency responsible for the implementation of the State Plan for the Child Care and Development Block Grant (CCDBG) Act of 1990 as amended by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, is responsible for supervising the activities of social services districts in the administration of the child care subsidy program; and

WHEREAS, OCFS, is responsible for the reception, care and placement of children placed with OCFS as juvenile delinquents or juvenile offenders pursuant to Article 3 of the Family Court Act; and

WHEREAS, DOH, as the single State agency responsible for the Medical Assistance Program under Title XIX of the Social Security Act and Title 11 of Article 5 of administration of the Medical Assistance Program in New York; and

WHEREAS, OCFS and DOH have a mutual interest, consistent with their respective statutory obligations in relation to child welfare and medical assistance programs, in the exchange data, including client specific information; and

WHEREAS, Subdivision 12 of Section 366 of the Social Services Law, as amended by the laws of 1994, authorizes the Commissioner of the Single State Agency for Medical Assistance to apply pursuant to subdivision (c) of Section 1915 of the Federal Social Security Act for waivers to provide Medical Assistance to persons under the age of twenty-one years as further defined in such subdivision; and

WHEREAS, in accordance with the provision of Title XIX of the Social Security Act and Title II of Article 5 of the Social Services law, the Single State Agency for Medical Assistance has submitted to the Secretary of the United States Department of Health and Human Services (“Secretary”) for approval three requests for waivers of certain requirements of the State Plan to implement a home and community-based program of services to address unmet health needs for certain children in foster care, and certain children who have been discharged from foster care but continue to be eligible for the waiver program; and

WHEREAS, each waiver request is related to a single, specific target group of children having either a severe emotional disturbance, a developmental disability or physical health issues; and

WHEREAS, the waivers shall be hereinafter referred to individually and collectively as the B2H waiver program; and

WHEREAS, it is the intent of OCFS and DOH to enter into this AGREEMENT that will provide for the exchange of data, including client specific information, to further the legitimate needs of each agency; more particularly to facilitate Medical eligibility for the population of children in foster care, children receiving adoption subsidies, children participating in any of the B2H waiver programs and children in the custody of OCFS monitoring of the provision of medical care and services to these populations, consistent with applicable confidentiality standards; the AGREEMENT addresses the needs for current and future exchange of data between OCFS and DOH.

NOW, THEREFORE, IT IS MUTUALLY AGREED AS FOLLOWS:

1. DOH will provide to OCFS Medicaid enrollment, coverage and child specific payment information related to children in foster care, children receiving adoption subsidies, children participating in any of the B2H waiver programs and children in the custody of OCFS as juvenile delinquents of juvenile offenders, including Medicaid Management Information System (MMIS) known as “EMedNY”, medical payments. The information will include:

- a) Name, Client Identification Number (CIN) Date of Birth (DOB) and all other identifying information;
  - b) Demographic data;
  - c) Medicaid authorization dates, types of coverage;
  - d) Restricted recipient and principal provider data; and
  - e) Family income and resources.
2. DOH will provide access to OCFS Medicaid information related to families receiving child care subsidy payments which includes the following:
- a) Name, Client Identification Number (CIN) Date of Birth) and all other identifying information;
  - b) Demographic Information
  - c) Family income and resources
3. OCFS will provide to DOH information related to children in foster care, children receiving adoption subsidies, children participating in any of the B2H waiver programs and children in the custody of OCFS as juvenile delinquents or juvenile offenders, who are receiving Medicaid. The information will include:
- a) Welfare Management System (WMS) data available through the Welfare Reporting and Tracking System (WRTS) including case related, case member and CIN related data;
  - b) Foster care placement data; and
  - c) WMS Medicaid Subsystem data.
4. OCFS and DOH will each designate a principal contact person within its agency to be responsible for the coordination of data exchange. Such person will also be the principal contact person for any future data requests. Each agency will use its best efforts to accommodate such requests consistent with applicable legal standards and administrative capability.
5. OCFS and DOH agree to maintain the confidentiality of client specific information received from the other agency consistent with applicable confidentiality standards, including Section 471 of the Social Security Act, Section 372 of the Social Services Law and 18 NYCRR Parts 357 and 465 in regard to foster care records, and Section 1902(a)(7) of the Social Security Act, Section 369(4) of the Social Services Law and the provisions of the Health Insurance Portability and Accountability Act.
6. This AGREEMENT may be amended upon the mutual consent of the parties.

IN WITNESS WHEREOF, the parties have hereunto signed this AGREEMENT on the day and year appearing opposite their respective signatures.

\_\_\_\_\_  
DATE

BY: \_\_\_\_\_  
Name  
Executive Deputy Director  
NYS Office of Family & Children Services

\_\_\_\_\_  
DATE

BY: \_\_\_\_\_  
Name  
Chief of Staff  
NYS Department of Health

## State of Colorado – Master Memorandum of Understanding

---

The following data sharing agreement is executed within the State of Colorado’s human services department for and between various state public assistance programs and the state’s Judicial Department. The agreement addresses the purposes, restrictions, roles and responsibilities, security, and other aspects of data protections relative to a joint effort to create a technology for information-sharing by all agencies of state government that operate programs of prevention, intervention and/or treatment for children and youth.

### INTERAGENCY

### MEMORANDUM OF UNDERSTANDING

between

**COLORADO DEPARTMENT OF PUBLIC HEALTH AND ENVIRONMENT**

and

**STATE OF COLORADO JUDICIAL DEPARTMENT**

This Memorandum of Understanding (hereinafter “MOU”) is made by and between the STATE OF COLORADO, acting by and through the COLORADO DEPARTMENT OF PUBLIC HEALTH AND ENVIRONMENT, whose address or principle place of business is 4300 Cherry Creek Drive South, Denver, CO 80246 (hereinafter “CDPHE”), and the STATE OF COLORADO JUDICIAL DEPARTMENT, a separate branch of state government, whose administrative office is located at 1301 Pennsylvania Street, Suite 300, Denver, CO 80203 (hereinafter “Judicial Department”). The Judicial Department and CDPHE may each be referred to herein as a “Party” or collectively as the “Parties”.

WHEREAS, the Colorado Legislature has enacted legislation at Section 25-20.5-101 *et seq*, as amended, C.R.S. (hereinafter the “Act”) intended to coordinate the several prevention, intervention, and treatment programs for children and youth operated through various divisions, departments and agencies within the executive branch; and

WHEREAS, the Colorado Legislature has created a Prevention Services Division (hereinafter the “Division”) within CDPHE to operate prevention and intervention programs, to oversee the provision of prevention, intervention, and treatment services and to ensure collaboration among such programs and the availability of services for children and youth; and

WHEREAS, the Division, as required by the Act at Section 25-20.5-105, has developed the “State Plan for Prevention, Intervention, and Treatment Services for Children and Youth” (hereinafter the “State Plan”), which applies to all prevention, intervention, and treatment programs that receive state and federal funds and are operated within the state, and has created the Colorado Prevention Leadership Council (hereinafter the “Council”) with representatives from each of the State executive branch agencies that fund prevention, intervention, and/or treatment services for children and youth, to serve as the interagency collaborative group; and

WHEREAS, the State Plan calls for development of the capability for sharing of information about children and youth among all the state agencies that conduct such programs for children and youth; and

WHEREAS, although the Act, at Section 25-20.5-109, specifically excludes from its provisions any program operated for juveniles by the “State Judicial System,” the Judicial Department desires to implement portions of the State Plan, and to work with the Council in a joint effort to create a technology for information-sharing by all agencies of state government that operate programs of prevention, intervention and/or treatment for children and youth.

NOW THEREFORE: in consideration of their mutual promises, stated below, the parties agree as follows;

1. Effective Date, Term and Termination. The effective date of this MOU is the date on which it has been signed by both Parties. This MOU shall continue indefinitely, until terminated by either Party. Either party may terminate this MOU upon written notice of termination, stating the effective date of such termination.
2. Obligations of Judicial Department. The Judicial Department agrees to:
  - a. Provide one or more representatives on the Council from Judicial Department divisions that provide prevention, intervention and/or treatment programs for children and youth.
  - b. Work to implement portions of the State Plan identified by the Judicial Department as being appropriate for its involvement.
  - c. Work with state executive branch agencies, through the Council and in collaboration with the Governor’s Office of Information Technology, to address the sharing of information from children and youth programs among all participating agencies from both the executive and judicial branches. This activity will include:
    - (1) Assist in the identification of:
      - (a) active data workgroups within or among state government agencies;
      - (b) information currently being collected from various state data systems and for what purposes it is collected;
      - (c) redundancies in data collected across the state government data systems;
      - (d) other necessary information to be shared and under what conditions.
    - (2) Provide Judicial Department representation on the Colorado Data Sharing and Utilization Group (“CDSUG”) of the Council that will explore technology solutions for information-sharing, and brief the State Court Administrator and executive branch leadership on these efforts, as well as on implementation strategies.
    - (3) Provide Judicial Department representation on the Children and Youth Sharing (“CCYIS”) Group, a subcommittee of the CDSUG to develop cross-system protocols utilizing and adapting the federal Guidelines for Juvenile Information Sharing (Office of Juvenile Justice and Delinquency Prevention, 2006).
  - d. Assist in the implementation of the “Colorado LINKS for Mental Health” *Children and Youth Behavioral Health Action Plan*, an initiative of the Council to create partnerships between state government agencies and community groups working in the children’s mental health system.
  - e. Attend the annual, or more frequent, meetings required by the Act at Section 25-20.5-107(6).
3. Obligations of the CDPHE.
  - a. Invite the State Court Administrator, or designee, to the annual, or more frequent, meetings required by the Act of Section 25-20.5-107(6) to review the activities and progress of the Division and its interaction with the prevention, intervention, and treatment programs provided by state agencies.
  - b. Provide for the cooperation of state executive branch agencies in the work of the information sharing project; and



4. The Judicial Department’s participation under this MOU and its implantation of some provisions of the State Plan do not constitute a waiver of the exception from all other provisions of the Act granted at Section 25-20.5-109, as amended, C.R.S.
5. Each party warrants that it possesses legal authority to enter into this MOU, and each person signing this MOU warrants that s/he possesses legal authority to execute the MOU on behalf of the Party that the person represents.
6. Subject to Public (Open) Records Act (Section 24-72-101, et seq., as amended C.R.S) if either Party obtains access to any records, files, or information of the other Party in connection with, or during the performance of, this MOU, then the said Party shall keep all such records, files, or information confidential and shall comply with all laws and regulations concerning the confidentiality of all such records, files, or information to the same extent as such laws and regulations apply to the other Party.

IN WITNESS WHEREOF, the Parties have executed this MOU effective in the dates written below.

STATE OF COLORADO  
JUDICIAL DEPARTMENT

STATE OF COLORADO  
Bill Ritter, Jr., Governor  
DEPARTMENT OF PUBLIC HEALTH  
AND ENVIRONMENT

By: \_\_\_\_\_

Name  
State Court Administrator

By: \_\_\_\_\_

Name  
Executive Director

## **ACF/Office of Child Support Enforcement – Security Agreement**

---

The following data sharing agreement is executed between each state child support agency and the federal Office of Child Support Enforcement. The agreement addresses the purposes, restrictions, roles and responsibilities, security, and other aspects of data protections relative to the request, use, and confidentiality and protection of data sources such as from the Federal Parent Locator Service, the National Directory of New Hires, Federal Case Registry, and Federal Tax Offset information shared electronically by the federal Office of Child Support Enforcement with the state child support agencies on a routine basis.

### **SECURITY AGREEMENT**

**U.S. Department of Health and Human Services**

**Administration of Children and Families**

**Office of Child Support Enforcement**

**and**

**State Agency Administering the Child Support Program**

## **I. PURPOSE AND EFFECT OF THIS SECURITY AGREEMENT**

The purpose of this security agreement is to specify the management, operational and technical security controls that the state agency administering the Child Support (CS) Program shall have in place to ensure the security of Federal Parent Locator Service (FPLS) information and CS program information and the information systems that transmit, store and process FPLS information and CS program information.

By signing this security agreement, the state CS agency agrees to comply with the applicable security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 USC 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS) and the federal Office of Child Support Enforcement (OCSE). The state CS agency also agrees to use FPLS information and CS confidential program information solely for the authorized purposes in accordance with the terms in this security agreement between the state CS agency and OCSE. The state CS agency requests submitted to the FPLS are made solely to locate a parent for the purpose of establishing paternity, securing child support, or where applicable, to locate a parent in a parental kidnapping case, establish or enforce a child custody or visitation order, and for other purposes specified in federal law and regulations. The information exchanged between state CS agencies and all other state program information may only be used for authorized purposes under federal law and regulations (see 45 Code of Federal Regulations (CFR) 303.21) and must be protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

## Appendix B.

In this security agreement (including the addendum), “state CS agency” means the single and separate state agency responsible and accountable for the operation of the child support program under title IV-D of the Social Security Act (see 45 CFR 302.12(a)) and required to operate child support data systems under 42 U.S.C. 454(3), (24), (26), (27) and (28) as a condition of federal funding, and its agents and designees, including all of the individuals and entities described in this agreement. “Information” and “data” means all forms of confidential information or data described in this agreement.

In this security agreement (including the addendum), “State CS Director or Designee” means the individual designated to administer the state CS program.

This security agreement is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of the state CS agency, including, but not limited to, state employees and contractors working with FPLS information and CS confidential program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services’ data centers, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information.

Information originally transmitted from the FPLS to the state CS agency does not lose its character as FPLS information but remains FPLS information until its destruction; nor do the safeguarding requirements end when the information is transmitted to state CS agencies or other entities.

This security agreement is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system which locates employment, income, asset and home address information on parents in child support cases for state CS agencies. The NDNH contains new hire (W-4), quarterly wage (QW) and unemployment insurance (UI) information on employees in both the public and private sector. The Debtor File contains personal information in identifiable form including names, Social Security numbers, arrearages, and other confidential information. The FCR collects and maintains records provided by state CS agency registries, which include abstracts of support orders and information from child support cases with name, Social Security number, state case identification number, state Federal Information Processing Standard (FIPS) code, county code, case type, sex, date of birth, mother’s maiden name, father’s name, participant type (custodial party, noncustodial parent, putative father, child), family violence indicator (domestic violence or child abuse), order indicator, locate request type and requested locate source.

This security agreement is applicable to all CS program information designated as confidential under federal law or regulation because the information relates to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. *Ref. 45 Code of Federal Regulations (CFR) 303.21(a).*

If the information system that stores, processes and/or transmits the FPLS information and/or CS confidential program information is not under the direct management of the state CS agency, the state CS agency shall execute the attached security addendum to this security agreement. As an agent or designee of the CS agency, the organization that provides information system services to the state CS agency shall comply with all management, operational and technical controls listed in this security agreement.

This security agreement may be updated to address changes in processes or technologies, as well as new or revised federal security requirements and guidelines. In such instances, OCSE shall provide the state CS agency with written notification of such changes and require written assurance by the state CS agency that it shall comply with new or revised security requirements.

If OCSE determines that the security or privacy of FPLS information or any CS program information is at risk, OCSE will work to support the state CS agency's efforts to provide a written description of their corrective actions or develop a Plan of Action and Milestones (POA&M) to address vulnerabilities and correct deficiencies.

This agreement shall be effective on the later of the dates on which the authorized officials of the CS agency and the agency designated to provide information services to the CS agency sign the security agreement. This security agreement shall remain in effect for a period of five years.

## II. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

The state CS agency shall comply with the applicable provisions of the *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P)* and the *Automated Systems for Child Support Enforcement: A Guide for States*, dated August 2009 (Federal Certification Guide). The following requirements are drawn from these documents. The state CS agency was provided a copy of these documents October 2013.

The security requirements with which the state CS agency shall comply are presented in three categories: management, operational, and technical. The state CS agency shall also comply with four additional requirements: Retention and Disposition Requirements; Breach Reporting and Notification Responsibility; Security Certification; and Audit Requirements.

### A. MANAGEMENT SECURITY CONTROLS

1. The state CS agency shall establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to FPLS information and CS program information.

**Policy/Requirements Traceability:** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, PL-4, PS-6, PS-8; 45 CFR 307.13(a) and (b); 45 CFR 95.621(f); 45 CFR 307.10(b)(11); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

2. The state CS agency shall advise all authorized personnel who will access FPLS information and CS program information of the confidentiality of the FPLS information and CS program

information, the safeguards required to protect the FPLS information and CS program information, and the civil and criminal sanctions for non-compliance contained in the applicable federal and state laws.

**Policy/Requirements Traceability:** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, PL-4, PS-6, PS-8; 42 U.S.C. 654 (26); 45 CFR 95.621(f); 45 CFR 307.10(b)(11); 45 CFR 307.11(b)(2)(iii); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

3. The state CS agency shall prohibit the use of non-state furnished equipment to access FPLS information and CS program information without specific written authorization for use of the equipment from the appropriate state CS agency representatives.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, POES

4. The state CS agency shall require that personnel accessing FPLS information remotely, for example telecommuting, adhere to all the security and privacy safeguarding requirements provided in this security agreement. State and non-state furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Prior to electronic connection to state CS agency systems, the state CS agency shall scan the state and non-state furnished equipment to ensure compliance with a set of standards developed by the state CS agency. All connections shall be through a Network Access Control solution and all data in transit between the remote location and the state CS agency shall be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Equipment that may be authorized includes mobile devices which meet the HHS standards related to such devices. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, POES; OMB M-06-16, *Protection of Sensitive Agency Information*; OMB-M-07-16; NIST SP 800-53 Rev 3, AC-17, AC-20; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

The state CS agency shall require that personnel accessing CS confidential program information remotely, for example telecommuting, adhere to the applicable security and privacy safeguarding requirements provided in this security agreement. State and non-state furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Prior to connection to state CS agency resources, the state CS agency shall use appropriate measures to ensure the state and non-state furnished equipment comply with a set of standards developed by the state CS agency. Equipment that may be authorized includes mobile devices which meet the state agency standards related to such devices. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, POES; OMB M-06-16, *Protection of Sensitive Agency Information*; OMB-M-07-16; NIST SP 800-53 Rev 3, AC-17, AC-20; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

5. The state CS agency shall implement an effective continuous monitoring strategy and program to ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing FPLS information and CS confidential program information.

**Policy/Requirements Traceability:** NIST SP 800-53 Rev 3, CA-7; NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H3 and H4.

6. The state CS agency system shall meet all requirements set forth in the Federal Certification Guide, *Automated Systems for Child Support Enforcement: A Guide for State*, Section H, “Security and Privacy”.

**Policy/Requirements Traceability:** 45 CFR 302.85(a)(1); Federal Certification Guide, Chapter III, Section H, “Security and Privacy.”

7. The state CS agency shall document and report to OCSE’s Division of State and Tribal Systems (DSTS) any significant changes to the state CS agency’s security procedures and provide copies of the appropriate updated security manual, disaster recovery plan, and risk analysis plan upon request.

**Policy/Requirements Traceability:** 45 CFR 95.621(f); 45 CFR 307.13; OCSE Action Transmittal (AT)-03-03; and Federal Certification Guide, Chapter III, Sections H1, H3, H4, and H5.

8. The state CS agency security office shall conduct and/or participate in the biennial system security reviews of installations involved in the administration of the state CS agency program which, at a minimum, includes evaluations of physical and data security operating procedures, and personnel practices, in accordance with 45 CFR Part 95.621(f). The state CS agency shall make biennial system security reviews available to DSTS, upon request.

**Policy/Requirements Traceability:** 45 CFR Part 95.621(f); and, OCSE Action Transmittal (AT)-03-03.

## **B. OPERATIONAL SECURITY CONTROLS**

1. The state CS agency shall restrict access to, and disclosure of, the FPLS information to

authorized personnel who need the FPLS information to perform their official duties in connection with the authorized purposes specified in the security agreement. The state CS agency requests submitted to the FPLS are made solely to locate a parent for the purpose of establishing parentage, or establishing, setting the amount of, modifying or enforcing child support obligations, or where applicable, to locate a parent in a parental kidnapping case, establish or enforce a child custody or visitation order, and for other purposes specified in federal law and regulations. The information exchanged between state CS agencies shall be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

**Policy/Requirements Traceability:** Privacy Act 5 U.S.C. 552a (b)(1); 45 CFR 303.3(b)(6); 45 CFR 303.21; and, 45 CFR 307.13(a) and (b).

The state CS agency shall restrict access to, and disclosure of, the CS program information to authorized personnel who need the CS confidential program information to perform their official duties in connection with the authorized purposes specified in the security agreement. The information exchanged between state CS agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

**Policy/Requirements Traceability:** 45 CFR 95.621(f)(2); CFR 303.21(a)(1); 45 CFR 307.13(a) and (b); and Federal Certification Guide, Chapter III, H2.

2. The state CS agency shall label printed reports containing FPLS information and CS confidential program information to denote the level of sensitivity of the information and limitations on distribution. The state CS agency shall maintain printed reports in a locked container when not in use and never transport FPLS information and CS program information off state CS agency premises unless required for a purpose approved by the state CS Director or designee. When no longer needed, in accordance with the retention and disposition requirements in section III of this security agreement, the state CS agency shall destroy printed reports by shredding or burning.

**Policy/Requirements Traceability:** *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook*, MP, MS; NIST SP 800-53 Rev 3, MP-3, MP-4, MP-5, MP-6; and 45 CFR 307.13(a) and (b).

3. The state CS agency shall deliver security and privacy awareness training for authorized personnel. The training shall include information about the responsibility of such personnel for proper use and protection of FPLS information and CS program information, recognizing and reporting potential indicators of insider threat, and the possible federal and state sanctions for misuse. All personnel shall receive security and privacy awareness training prior to accessing FPLS information and CS program information and at least annually thereafter. Such training

shall address the federal Privacy Act and other federal and state laws governing use and misuse of FPLS information and CS program information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, AT; FISMA; OMB Circular A-130; OMB M-07-16; NIST SP 800-53 Rev 3, AT-2, AT-3; 42 U.S.C. 654a(d); 45 CFR 307.13(c) and (d); and Federal Certification Guide, Chapter III, H2.

4. The state CS agency personnel with authorized access to the FPLS information and CS program information shall sign (either in handwritten or electronic form) non-disclosure agreements, rules of behavior, or equivalent documents. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the FPLS information and CS confidential program information may be used by the state CS agency and the federal and state civil and criminal penalties for unauthorized use.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, USE; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, PS-6; 42 U.S.C. 654a(d); 45 CFR 307.13(d); and Federal Certification Guide, Chapter III, H2.

5. The state CS agency shall maintain records of authorized personnel with access to the FPLS information and CS confidential program information. The records shall contain a copy of each individual's signed non-disclosure agreement, rules of behavior, or equivalent document and proof of the individual's participation in security and privacy awareness training. The state CS agency shall make such records available to OCSE within two working days of a request for such records.

**Policy/Requirements Traceability:** NIST SP 800-53 Rev 3, AT-4.

6. The state CS agency shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving personal information), or suspected incidents involving FPLS information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state CS Director or designee shall notify the FPLS Information Systems Security Officer (ISSO) designated on this security agreement of suspected or confirmed incidents. The requirement for the state CS Director or designee to report suspected or confirmed incidents involving FPLS information to OCSE exists in addition to, not in lieu of, any state CS agency requirements to report to any other reporting agencies. The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting or processing FPLS information and to report suspected or confirmed incidents of such information to the state CS Director or designee.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, IR; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, IR-6; and Federal Certification Guide, Chapter III, H2.

The state CS agency shall have appropriate procedures in place to report security or privacy



incidents (unauthorized disclosure or use involving personal information), or suspected incidents involving CS confidential program information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state CS Director or designee shall notify the FPLS Information Systems Security Officer (ISSO) designated on this security agreement of suspected or confirmed incidents involving 1) an unauthorized individual who obtains access, either physical or virtual, to the information systems of the state CS agency, or 2) the unauthorized disclosure or use of personal information pertaining to multiple individuals. For privacy incidents arising out of the ordinary course of business involving the unauthorized disclosure or use of CS program information pertaining to one individual, the state CS director or designee must ensure prompt and adequate investigation and mitigation of the incident. The requirement for the state CS Director or designee to report suspected or confirmed incidents involving CS program information to OCSE exists in addition to, and not in lieu of, any state CS agency requirements to report to any other reporting agencies. The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting, or processing CS program information and to report suspected or confirmed incidents of such information to the state CS Director or designee.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, IR; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, IR-6; and Federal Certification Guide, Chapter III, H2

7. The state CS agency shall maintain a list of personnel authorized to access facilities and systems processing sensitive data, including FPLS information and CS program information. The state CS agency shall control access to facilities and systems wherever sensitive information is processed. Designated officials shall review and approve the access list and authorization credentials initially, and periodically thereafter, but no less often than annually.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, PE; NIST SP 800-53 Rev 3, AC-2, PE-2; 45 CFR 95.621(f); 45 CFR 307.13(b); and Federal Certification Guide, Chapter III, H2.

8. The state CS agency shall use locks and other protective measures at all physical access points (including designated entry/exit points) to prevent unauthorized access to computer and support areas containing FPLS information and CS confidential program information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, PE; NIST SP 800-53 Rev 3, PE-3; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2.

9. The state CS agency shall store all FPLS information and CS confidential program information provided pursuant to this security agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

**Policy/Requirements Traceability:** *HHS-OCIO Policy for IS2P Handbook*, PE; NIST SP 800-53 Rev 3, PE-2, PE-3; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2.

10. The state CS agency shall prohibit FPLS information from being copied to, and stored on, digital media unless encrypted at the disk or device level, using a FIPS 140-2 compliant product. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook, NCRTP; OMB M-07-16; FIPS 140-2, Security Requirements for Cryptographic Modules; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2.*

The state CS agency shall ensure that appropriate measures developed by the state CS agency are in place to protect CS confidential program information that is copied to, and stored on, digital media.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook, NCRTP; OMB M-07-16; FIPS 140-2, Security Requirements for Cryptographic Modules; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2.*

### C. TECHNICAL SECURITY CONTROLS

1. The state CS agency shall utilize and maintain technological (logical) access controls that limit access to FPLS information and CS confidential program information to only those personnel who are authorized for such access based on their official duties and identified in the records maintained by the state CS agency pursuant to Section II.B.5 and II.B.7 of this security agreement.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook, AC; NIST SP 800-53 Rev 3, AC-2; U.S.C. 654a(d); 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.*

2. The state CS agency shall prevent browsing with technical controls that limit access to FPLS information and CS confidential program information to assigned cases and areas of responsibility, or equivalent compensatory controls approved in writing by OCSE.

**Policy/Requirements Traceability:** *NIST SP 800-53 Rev 3, AC-3; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.*

3. The state CS agency shall transmit and store all FPLS information provided pursuant to this security agreement in a manner that safeguards the information and prohibits unauthorized access. The state CS agency and OCSE shall exchange CS confidential program information via a mutually approved and secure data transfer method which utilizes FIPS 140-2 encryption standards.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, MP; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, MP-4, SC-8, SC-9, SC-33; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

The state CS agency shall transmit and store all CS confidential program information pursuant to this security agreement in a manner that safeguards the information and prohibits unauthorized access. The state CS agency shall use appropriate measures developed by the state CS agency when exchanging CS confidential program information among other state CS agencies.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, MP; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, MP-4, SC-8, SC-9, SC-33; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

4. Except as described in Sections II.A.4 and II.C.10 or elsewhere in this agreement, the state CS agency shall prohibit the use of digital media and computing and communications devices resident in commercial or public facilities such as hotels, convention centers, and airports, from transmitting and/or storing FPLS information and CS confidential program information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, POES; NIST SP 800-53 Rev 3, AC-19, CM-8; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

5. The state CS agency shall prohibit remote access to FPLS information, except through the use of a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication, as required by the federal Office of Management and Budget Memorandum 06-16 (OMB M-06-16). The state CS agency shall control remote access through a limited number of managed access control points. If the state CS agency cannot provide two-factor authentication, the state CS agency shall submit to OCSE a written description of compensating controls, subject to written approval by OCSE prior to allowing remote access.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, RMT, IA; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, AC-17, IA-2, SC-8, SC-9.

The state CS agency shall prohibit remote access to CS confidential program information, except through the use of appropriate measures developed by the state CS agency. The state CS agency shall control remote access through a limited number of managed access control points.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, RMT, IA; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, AC-17, IA-2, SC-8, SC-9; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

6. The state CS agency shall utilize a time-out function for remote access and mobile devices that require a user to re-authenticate after no more than 30 minutes of inactivity. See Sections II.A.3, II.A.4, and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, RMT; OMB M-06-16; OMB M-07-16; and Federal Certification Guide, Chapter III, H2.

7. The state CS agency shall maintain a fully automated audit trail system with audit records for FPLS information that, at a minimum, collect data associated with each query transaction to its initiator, capture date and time of system events and types of events. The audit trail system shall protect data and the audit tool from addition, modification, and/or deletion and should be regularly reviewed/analyzed for indications of inappropriate or unusual activity. The state agency shall retain the audit logs for a period of five years to support security incident investigations.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, AU; NIST SP 800-53 Rev 3, AU-2, AU-3, AU-6, AU-8, AU-9, AU-11; and Federal Certification Guide, Chapter III, Sections H2 and H3.

The state CS agency shall maintain a fully automated audit trail system with audit records for CS confidential program information that complies with provisions of the Federal Certification Guide, *Automated Systems for Child Support Enforcement: A Guide for States*, dated August 2009. The state agency shall retain the audit logs for a period of five years to support security incident investigations.

**Policy/Requirements Traceability:** 42 U.S.C. 654a(d)(3); 45 CFR 95.621(f); 45 CFR 307.13(b); and Federal Certification Guide, Chapter III, Sections H2, H3 and H4.

8. The state CS agency shall log each computer readable data extract (secondary store or file with duplicate CS confidential program information) from any databases holding FPLS information and verify that each extract has been erased within 90 days after completing required use. If use of the extract is still required to accomplish a purpose authorized pursuant to this security agreement and complies with the retention and disposition requirements in Section III of this security agreement, the state CS agency shall request permission, in writing, to keep the extract for a defined period of time, subject to OCSE's written approval.

**Policy/Requirements Traceability:** OMB M-06-16; OMB M-07-16.

The state CS agency shall use appropriate measures developed by the state CS agency to log each computer readable data extract (secondary store or file with duplicate CS program

information) from any databases holding CS confidential program information and verify that each extract has been erased after completing required use.

**Policy/Requirements Traceability:** OMB M-06-16; OMB M-07-16; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4.

9. The state CS agency shall erase electronic records after completing authorized use in accordance with the retention and disposition requirements in section III of this security agreement.

**Policy/Requirements Traceability:** Privacy Act 5 U.S.C. 552a; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4.

10. The state CS agency shall implement a Network Access Control (NAC) (also known as Network Admission Control) solution in conjunction with a virtual private network (VPN) option to enforce security policy compliance on all state and non-state devices that attempt to gain access to, or use, FPLS information. The state CS agency shall use a NAC solution to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users before they can access the network. The NAC solution chosen or employed shall be capable of evaluating whether remote machines are compliant with security policies through host(s) Integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the state enterprise environment. In addition, functionality that allows automatic execution of code shall be disabled. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record/report on users' access and presence on the state network. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, S-RMT.1; NIST SP 800-53 Rev 3, AC-17, AC-20, IA-2, IA-3; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4.

The state CS agency shall implement appropriate measures developed by the state CS agency to enforce security policy compliance (such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the state enterprise environment) on all state and non-state devices that attempt to gain remote access to, or use, CS confidential program information. In addition, functionality that allows automatic execution of code shall be disabled. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record/report on users' access and presence on the state network. See Section II.A.3 and II.C.4 of this security agreement for additional information.

**Policy/Requirements Traceability:** *HHS OCIO Policy for IS2P Handbook*, S-RMT.1; NIST SP 800-53 Rev 3, AC-17, AC-20, IA-2, IA-3; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2.

### **III. RETENTION AND DISPOSITION REQUIREMENTS**

The state CS agency shall erase FPLS information and CS program information when data is no longer required for authorized purposes. FPLS information and CS confidential program information in an individual's case file should be safeguarded per the security requirements of this security agreement. FPLS information and CS confidential program information that is made part of an individual's case file may be retained in the individual's case file based on state CS agency's rules and procedures for case file retention.

### **IV. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY**

Upon disclosure of FPLS information from OCSE or disclosure of CS confidential program information from another state or tribe to the state CS agency, the state CS agency is the responsible party in the event of a breach or suspected breach of the information.

Except as otherwise provided in Section II.B.6, if the state CS agency knows or suspects FPLS or CS confidential program information has been breached, in either electronic or physical form, the state CS agency:

1. alerts the FPLS ISSO designated on this security agreement immediately upon discovery, but in no case later than one hour after discovery of the incident
2. follows the state CS agency procedures for responding to a data breach
3. reports the results of the investigation, mitigation, and resolution to the FPLS ISSO.

The state CS Director or designee is responsible for all reporting, notification, and mitigation activities as well as the associated costs. Reporting, notification and mitigation activities include but are not limited to: investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; communicating with any third parties, including the media, as necessary; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the breach of FPLS information and CS confidential program information; performing any necessary follow-up activities to correct the vulnerability that allowed the breach; and any other activities, as required by OCSE.

The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting or processing FPLS information and CS confidential program information to report confirmed or suspected incidents of such information to the state CS Director or designee.

## V. SECURITY CERTIFICATION

### A. Annual Certification Statement

The state CS agency shall certify annually that it continues to comply with the terms and requirements in this security agreement by submitting a Certification Statement to OCSE each year by March 31.

### B. Independent Security Assessment

Every five years, the state CS agency shall arrange for an independent security assessment to be conducted on the business processes involving FPLS information and CS program information and the computer systems storing and processing FPLS information and CS program information. The independent security assessment must have been conducted by an unbiased, outside entity and must include information on the management, operational and technical security controls defined within this security agreement. The independent security assessment must also include detailed findings (if any) and recommendations to improve the state CS agency's plans, procedures and practices. The state CS agency shall make such a report available to OCSE upon request.

The following assessments are acceptable:

- Internal Revenue Service Safeguard Review Report;
- Social Security Administration Independent Validation and Verification;
- A review conducted by an independent state auditing agency such as the State Office of the Inspector General; and,
- A review conducted by an independent auditing firm hired by the state agency.

The results of these independent security assessments must be incorporated into the state CS agency's respective reporting in the state's Biennial Security Review Report as required by federal regulations at 45 CFR 95.621. If major organizational, system framework, hardware, and operating software changes have taken place since the previous independent security assessment, a new independent security assessment must be conducted within six (6) months of the change. The state CS agency shall make such reports available to OCSE, upon request.

**Policy/Requirements Traceability:** OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(f)(3) and (6); and 45 CFR 305.60

## VI. AUDIT REQUIREMENTS

OCSE's Divisions of Federal Systems and State and Tribal Systems, and Office of Audit, reserve the right to audit the state CS agency or make other provisions to ensure that the state CS agency is maintaining adequate safeguards to protect the FPLS information and CS confidential program information. Audits ensure that the security policies, practices and procedures required by OCSE are in place and to assess the completeness, authenticity, reliability, accuracy and security of information and the systems used to process the data within the state CS agency.

**Policy/Requirements Traceability:** OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(a)(b) and (c); and, 45 CFR 305.60.



## VII. PERSONS TO CONTACT

- A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement security contact is:

Linda Boyer, FPLS Information System Security Officer  
Division of Federal Systems  
Office of Child Support Enforcement  
Administration for Children and Families  
370 L'Enfant Promenade, SW, 4<sup>th</sup> Floor  
Washington, DC 20447  
Telephone: 202-401-5410  
Fax: 202-401-5558  
E-mail: linda.boyer@acf.hhs.gov

- B. The state CS agency program contact is:

[NAME AND TITLE]  
[NAME OF DEPARTMENT]  
[NAME OF PROGRAM]  
[NAME OF AGENCY]  
[ADDRESS OF AGENCY]  
Telephone:  
Fax:  
E-mail:

- C. The state CS agency systems contact is:

[NAME AND TITLE]  
[NAME OF DEPARTMENT]  
[NAME OF PROGRAM]  
[NAME OF AGENCY]  
[ADDRESS OF AGENCY]  
Telephone:  
Fax:  
E-mail:

D. The state CS agency security contact is:

[NAME AND TITLE]  
[NAME OF DEPARTMENT]  
[NAME OF PROGRAM]  
[NAME OF AGENCY]  
[ADDRESS OF AGENCY]  
Telephone:  
Fax:  
E-mail:

E. The state CS agency data center contact is:

[NAME AND TITLE]  
[NAME OF DEPARTMENT]  
[NAME OF PROGRAM]  
[NAME OF AGENCY]  
[ADDRESS OF AGENCY]  
Telephone:  
Fax:  
E-mail:

F: The state's designated Automated Data Processing (ADP) security officer, per federal regulations at 45 CFR 95.621, is:

[NAME AND TITLE]  
[NAME OF DEPARTMENT]  
[NAME OF PROGRAM]  
[NAME OF AGENCY]  
[ADDRESS OF AGENCY]  
Telephone:  
Fax:  
E-mail:

## VIII. APPROVALS

In witness whereof, the parties hereby approve this security agreement.

- A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement Program Official**

<b>Linda Boyer</b> FPLS Information Systems Security Officer	<b>Date</b>
<b>Vicki Turetsky</b> Commissioner	<b>Date</b>

**B. State CS Director or designee (see note)**

<p><b>[Name of State CS Director or designee]</b></p> <p><b>[Title of State CS Director or designee]</b></p>	<p><b>Date</b></p>

**C. State CS agency Information Systems Security Official (see note)**

<p><b>[Name of State CS agency Information Systems Security Official]</b></p> <p><b>[Title of State CS agency Information Systems Security Authorized Official]</b></p>	<p><b>Date</b></p>

**NOTE:** If the state CS director (or designee) in subsection VIII.B, or the state CS agency Information Systems Security Official in subsection VIII.C, no longer serves in the designated capacity, the individual assuming the responsibilities of either individual must sign the appropriate signature box and submit the page containing the signature to OCSE.

## SECURITY ADDENDUM

**State Agency Administering the Child Support Program**

**and**

**[Organization Providing Information Technology Services]**

### **PURPOSE AND EFFECT OF THIS SECURITY ADDENDUM**

The purpose of this security addendum is to affirm that any organization operating an information system that houses, processes or transmits Federal Parent Locator Service (FPLS) information and child support (CS) program information on behalf of the state CS agency shall comply with all management, operational and technical controls listed in the security agreement.

This security addendum is applicable to all CS confidential program information, which means confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. *Ref. 45 Code of Federal Regulations (CFR) 303.21(a)*

This security addendum is also applicable to FPLS information, which consists of the National Directory of New Hire (NDNH), Debtor File, Federal Case Registry (FCR) and all associated applications and resources. The NDNH, Debtor File and FCR are components of an automated national information system which locates employment, income, asset and home address information on parents in child support cases for state CS agencies. The NDNH contains new hire (W-4), quarterly wage (QW) and unemployment insurance (UI) information on employees in both the public and private sector. The Debtor File contains personal information in identifiable form including names, Social Security numbers, wages, and other private data. The FCR collects and maintains records provided by state CS registries, which include abstracts of support orders and information from child support cases with name, Social Security number, state case identification number, state Federal Information Processing Standard (FIPS) code, county code, case type, sex, date of birth, mother's maiden name, father's name, participant type (custodial party, noncustodial parent, putative father, child), family violence indicator (domestic violence or child abuse), order indicator, locate request type and requested locate source.

Organizations to which this addendum applies include contractors of the state CS agency or other internal or external organizations working on behalf of the state CS agency.

By signing this security addendum, the state CS agency agrees to ensure that the organization providing information system services complies with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), the U.S. Department of Health and Human Services (HHS), 42 United States Code (U.S.C.) 654(26), 42 U.S.C. 654a(d)(1)-(5) and the federal Office of Child Support Enforcement.

The organization providing information system services also agrees to protect FPLS information and CS program information against unauthorized access and to protect the privacy rights of individuals whose information is stored and processed within the information system supporting the CS program.

## **BREACH REPORTING AND NOTIFICATION RESPONSIBILITY**

Except as otherwise provided in Section II.B.6 of the Security agreement, in the case of a confirmed or suspected data breach involving FPLS information and/or CS program information, the organization providing information system services agrees to report the breach immediately upon discovery, but in no case later than one hour after discovery of the incident, to the state CS Director or designee designated on this security addendum. See Security Agreement, Section IV for additional information.

## **INFORMATION SEGREGATION REQUIREMENTS**

The organization providing information system services shall protect the FPLS information and state CS confidential program information and segregate it from the provider's infrastructure to ensure that only authorized personnel have access to the FPLS information and state CS program information.

## **AUDIT REQUIREMENTS**

OCSE's Divisions of Federal Systems, State and Tribal Systems, and Office of Audit reserve the right to audit the state CS agency and any organization providing information system services to the state CS agency or make other provisions to ensure that the state CS agency is maintaining adequate safeguards to protect the FPLS information and CS program information. Audits ensure that the security policies, practices and procedures required by OCSE are in place and to assess the completeness, authenticity, reliability, accuracy and security of information and the systems used to process the data within the state CS agency and any organization providing information system services to the state CS agency.

**Policy/Requirements Traceability:** OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(a)(b) and (c); and 45 CFR 305.60

Approved subject to and as qualified by the Plan of Action and Milestones, attached hereto and incorporated herein.

**APPROVALS**

In witness whereof, the parties hereby approve this security addendum.

**A. State CS Director or designee (see note)**

[Name of State CS Director or designee]	
[Title of State CS Director or designee]	Date

**B. State CS agency Information Systems Security Official (see note)**

[Name of State CS Agency Information Systems Security Authorized Official]	
[Title of State CS Agency Information Systems Security Authorized Official]	Date

**C. [Organization] Information Systems Security Official (see note)**

[Name of Information Systems Security Authorized Official]	
[Title of Information Systems Security Authorized Official]	Date

**NOTE:** If the state CS director (or designee) in Section A, or the state CS agency Information Systems Security Official in Section B, or the [Organization] Information Systems Security Official in Section C no longer serves in the designated capacity, the individual assuming the responsibilities of the individual must sign the appropriate signature box and have the state CS agency submit the page containing the signature to OCSE.

## Montgomery County, Maryland – Notice of Privacy Practices

---

The following notice is executed between the Montgomery County Department of Health and Human Services and clients to explain the county's data sharing and privacy practices and rules relative to client information used to determine services eligibility and delivery. This is an "opt-in" data sharing practice.

### **MONTGOMERY COUNTY DEPARTMENT OF HEALTH AND HUMAN SERVICES 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.

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 of Privacy Practices* and to follow it. We have the right to change our privacy practices and the terms of this *Notice* and to make the changes effective for all health and other personal information we maintain. We will let you know about any changes to our privacy practices at your next visit to our offices. A current version of our *Notice* will be available in our waiting rooms and on the DHHS website at [www.montgomerycountymd.gov](http://www.montgomerycountymd.gov)

## How We May Use and Disclose Information *without* your Written Permission

- **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. 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.

DHHS staff in the following programs will not share program information about you with staff who are providing you with services in other programs without your written permission:

- Alcohol and Substance Abuse Treatment Programs
- Domestic Abuse, Sexual Assault or Victim's Assistance Programs
- DHHS programs that maintain records that are considered "education records" under the Family Education Rights and Privacy Act of 1974.

DHHS staff 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.

- **For payment:** We may use or disclose health and other personal information about you as necessary to obtain payment for the health and mental health services you receive. 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 that you receive 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 to 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 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.
- **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.

- **As Required by Law:** If a law or regulation requires that we disclose your health or other personal information, we must do so.

## How We May Use or Disclose Alcohol or Substance Abuse Program Information

The confidentiality of alcohol and drug abuse treatment records is protected by federal law and regulations. Generally, we will not use or disclose information related to your alcohol or drug abuse treatment 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.

## Your Rights Regarding your Information

### You have the right to:

- Obtain a copy of this Notice of Privacy Practices. 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 we made this decision and how you can ask for a review of the denial or file a complaint.
- Make a request that your information be amended (changed) if you feel the information we have is wrong 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 and inform you about your right to give us a written statement disagreeing with the denial.
- Receive an accounting (a detailed listing) of disclosures we have made of your health information after April 14, 2003. 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 use or disclose 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.
- To file a complaint or report a problem.

## **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 at the end of this notice. 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.

## **To File a Complaint or Report a Problem**

To file a complaint or report a problem about how we have used or disclosed information about you, contact our Privacy Officer at the following address:

Privacy Officer  
Montgomery County Department of Health and Human Services  
401 Hungerford Drive  
Rockville, MD 20850  
240-777-3050 (Voice) 240-777-1398 (TTY)

We will not take any action against you for filing a complaint or for cooperating with an investigation, and the benefits and services you receive will not be negatively affected in any way.

If your complaint or concerns relate to how we have used or disclosed your *health* information, you may also contact:

Region III, Office for Civil Rights, U.S. Department of Health and Human Services  
150 S. Independence Mall West, Suite 372  
Public Ledger Building, Philadelphia, PA 19106-9111  
215-861-4441 (voice) 215-861-4441 (TDD) 1-800 368-1019 (Hotline)

## Montgomery County Department of Health and Human Services Notice of Privacy Practices Summary and Signature Page

### What is the Notice of Privacy Practices?

We are required by law to provide you with a notice of our privacy practices. Our complete *Notice of Privacy Practices* is attached. The purpose of the *Notice* is to inform you about:

- Our legal obligation to protect your information.
- How we will share your information without your written permission.
- Rights that you have related to your information.
- Who you can contact to ask questions, make a request, or file a complaint.

### How will we share your information?

Our Department provides a variety of health, income support and social services. To provide these services, we must ask you for personal information that may contain health, financial and other information that identifies you. We will keep your information safe and will only share it when the law permits us or requires us to do so. We will share your information as necessary to:

- Provide you with high quality and coordinated treatment and services.  
Example: Communicating information between programs to make referrals, determine eligibility or develop a care plan;
- Obtain payment for services. Example: Billing Medicaid;
- Manage our services and programs. Example: Reviewing the quality of the services you receive.

The attached *Notice* lists other reasons why we may share your information. If we need to share your information for reasons that are **not** listed, we will ask for your written permission. You have other rights related to your information that are listed on page 4 of the *Notice*.

### Contact Information:

If you have questions about our privacy practices, want to make a request related to your information, or have a privacy concern, contact the staff person who is working with you, or our Privacy Official at 240 777- 3050. Additional contact information is provided at the end of the *Notice*.

Acknowledgement of receipt of the complete *Notice*:

\_\_\_\_\_  
Client or Authorized Representative (Sign your name)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print your name

\_\_\_\_\_  
Signature of DHHS representative

\_\_\_\_\_  
Signature of interpreter/translator if applicable

If unable to get acknowledgement, specify why: \_\_\_\_\_

Page Intentionally Left Blank

# Glossary of Terms

---

ACA	Affordable Care Act
ACF	Administration for Children and Families (Department of Health and Human Services)
AFCARS	Adoption and Foster Care Analysis System
AFDC	Aid to Families with Dependent Children (Department of Health and Human Services)
CAPTA	Child Abuse Prevention and Treatment Act
CCDF	Child Care and Development Fund
CCYIS	Colorado Children and Youth Information Sharing Collaborative (State of Colorado)
CMA	Computer Matching Agreement
CMS	Centers for Medicaid and Medicare Services (Department of Health and Human Services)
COTS	Commercial Off-the-Shelf
CWPM	Child Welfare Policy Manual (Children's Bureau)
DCSE	Division of Child Support Enforcement (State of Delaware)
DSCYF	Department of Services for Children, Youth and Their Families (State of Delaware)
DSS	Department of Social Services (State of New York)
EBT	Electronic Benefit Transfer
FERPA	Family Educational Rights and Privacy Act
FCR	Family Case Registry
FIDM	Financial Institute Data Match
FNS	Food and Nutrition Service (Department of Agriculture)
FPLS	Federal Parent Locator Service (Administration for Children and Families)
GAO	Governmental Accountability Office
HHS	Department of Health and Human Services
HIE	Health Insurance Exchange
HIPAA	Health Information Portability and Accessibility Act
IEVS	Income and Eligibility Verification System
ILD	Independent Living Division
IRS	Internal Revenue Service (Department of the Treasury)
IM	Information Memorandum
LEA	Local Educational Agencies
LIHEAP	Low Income Energy Assistance Program (Administration for Children and Families)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSFIDM	Multistate Financial Institution Data Match
NAHIT	National Alliance for Health Information Technology
NCANDS	National Child Abuse and Neglect Data System
NCC	National Computing Center (Social Security Administration)
NDNH	National Directory of New Hires (Social Security Administration)
NIEM	National Information Exchange Model

OCSS	Office of Child Support Enforcement (Administration for Children and Families)
QIC	Quality Improvement Center
QRIS	Quality Rating and Improvement Systems
SACWIS	Statewide Automated Child Welfare Information Systems
SAMHSA	Substance Abuse and Mental Health Services Administration (Department of Health and Human Services)
SAVE	Systemic Alien Verification for Entitlements
SDNH	State Directory of New Hires
SDX	State Data Exchange
SSA	Social Security Act
SSI	Supplemental Security Income
SSIRS	Social Services Integrated Reporting System (State of California)
SSN	Social Security Number
SSO	Single Sign-On
SNAP	Supplemental Nutrition Assistance Program (Department of Agriculture)
SPLS	State Parent Locator Services (Administration for Children and Families)
SWICA	State Wage Information Collection Agency
TANF	Temporary Assistance for Needy Families (Department of Health and Human Services)
UI	Unemployment Insurance
UPMC	University of Pittsburg Medical Center
USCIS	United States Citizenship and Immigration Services (Department of Homeland Security)
USDA	Department of Agriculture



Page Intentionally Left Blank