Interagency Data Sharing Agreement
Between
Department of Children and Families
And
Department of Juvenile Justice

Agreement ID: DJJ-DCF 2015-01

This Agreement is made and entered into by and between the Florida Department of Children and Families, Office of Economic Self-Sufficiency (DCF) and the Department of Juvenile Justice (DJJ).

WHEREAS, the Agency for Health Care Administration (AHCA) receives data from DJJ pertaining to youth residing within residential commitment facilities, to determine the individuals receiving Medicaid benefits, and suspends the Medicaid coverage of the youth residing within the facility for thirty days or more;

WHEREAS, public assistance benefits are determined, in part, by the assistance group status, based on information submitted in the application process;

NOW THEREFORE, DCF must enter into an Interagency Data Sharing Agreement (Agreement) with DJJ to receive data pertaining to youth residing within residential commitment facilities in order to review and adjust public assistance benefits, as necessary for eligibility determination, to prevent overpayments of federal and state benefits and premature termination of public assistance benefits.

I. Purpose

The purpose of this Agreement is to establish the terms and conditions by which DJJ agrees to provide certain data to DCF on individuals who have been placed in a residential commitment facility.

The purpose of the data match is to identify and prevent overpayments and premature termination of federal and state benefits to public assistance recipients. DCF will complete a data match with the FLORIDA system to determine the individuals receiving public assistance benefits. When active cases are found, DCF will review the individual's participation status in the assistance group to determine the benefit level of the remaining members of the household. Because AHCA suspends the committed youth's status while in a commitment program, DCF will only use the data provided to determine the benefit level of the remaining members of the household.

II. Legal Authority

Section 39.523, Florida Statutes, Placement in residential group care
Chapter 419, Florida Statutes, Community Residential Homes
Chapter 985, Florida Statutes, Juvenile Justice; Interstate Compact on Juveniles

III. Definitions

A. Agreement Coordinators – the individuals appointed by the signatories as responsible for compliance with the activities identified herein.
B. Data Exchange – A process for taking data structured under a source database and mapping it to a target database, so that the target data is an accurate representation of the source data.
C. Covered Data - data covered by federal or state laws or regulations.

IV. Implementation

A. DCF agrees to provide the DJJ with a list of categorical data elements that encompass specific data it wishes to obtain from DJJ. The list of data elements is incorporated into this document as Exhibit A, Data Elements.

   1. Any revisions to Exhibit A shall require evidence of written mutual agreement between the Parties through the Agreement Coordinators, attaching the revised Exhibit A thereto and maintaining said evidence in the agreement file.

B. DCF agrees to restrict the transmission of the Covered Data received from DJJ using secure file transfer protocols to personnel who have a verifiable need to know in the performance of their official job duties.

C. DCF agrees to maintain a listing of personnel granted access privileges to the Covered Data pursuant to this Agreement and, upon request, make such information available to DJJ. At a minimum, the list shall include the user's name and title, User Identification (USERID), date access was granted/changed/deleted, and dates of initial security training and annual awareness training. This list shall be maintained at the information technology office of DCF and will also include the appropriate local technology officer's name and contact information. DCF agrees to maintain the Covered Data for a period of five (5) years after access has been terminated or until administrative purposes have been served, whichever is longer.

D. DCF agrees to abide by IT Security Awareness training provided by DCF. The training will comply with State information security statutes and rules.

E. DCF agrees that the Covered Data and Data Exchange obtained under this Agreement may not be disclosed by its employees verbally, electronically or in any other form except as specifically authorized by law or regulation. DCF agrees:

1. That any Covered Data provided to DCF pursuant to this Agreement will be used only in the performance of official duties and shall be disclosed only for those purposes as defined in this Agreement.

2. That the Covered Data obtained shall be stored in a place physically secure from access by unauthorized persons.

3. To safeguard access to the Covered Data in such a way that unauthorized persons cannot view, print, copy or retrieve the information by any means.

4. That DCF shall instruct all staff, employees, and personnel with access to the Covered Data including the confidentiality, safeguards, and requirements of this Agreement, and the provisions specified in Chapters 71A-1 and 71A-2,Florida Administrative Code, as well as Chapters 39, 119, 812, 815, 817, 839 or 877, or 985, Florida Statutes, and all applicable federal requirements. Initial and annual refresher IT Security Awareness training shall be required and documented.

5. That the confidentiality requirements of the Covered Data subject to this Agreement shall survive the expiration or termination of this Agreement.

6. To adhere to the confidentiality requirements stated herein, and promptly notify DJJ within twenty-four (24) hours of any breach of security related to Covered Data in its possession. To be responsible for full compliance with section 501.171, F.S., if applicable, in the event of a breach of security concerning confidential personal information in its possession received from one another, including but not limited to, providing notification to affected persons. To provide any such breach notification, if applicable, to DJJ for prior review and approval of the contents of the notice.

F. DJJ agrees to provide a monthly file consisting of first, last, and middle names of youth who have been committed to a residential commitment facility for thirty (30) days or more, along with youth social security numbers, admission dates, birthdates, sex, and actual release dates. For youth who have been admitted but not yet released, the actual release date field will be blank. The data shall be provided to DCF on a monthly basis prior to the tenth of each month, unless the parties mutually agree at a later date that a more frequent (but not less frequent) exchange schedule would be desirable with regards to the State ensuring adequate controls over access to benefits.

G. DCF shall ensure the adequacy of security controls for collecting, processing, transmitting and storing Covered Data in leased, procured or developed systems and technologies, including sub-components as long as the Covered Data exists in the systems. In any developed system or technology or subcomponent thereof, including views, prints or copies of the Covered Data,

a notice shall be provided to the user that the Covered Data is confidential and that users of the system shall be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. On-line systems shall require an acknowledgement and all views and prints shall contain the same statement. The violations of such confidential information security are addressed under Chapters 39, 119, 812, 815, 817, 839, or 877, or 985, Florida Statutes, and applicable Federal laws.

H. The following summary of key security standards is applicable to the Covered Data, in accordance with federal or state laws or regulations. The following list is not intended to be, and is not, exhaustive. DCF will comply with all security requirements related to Covered Data provided to, or collected by, DCF acting on behalf of DJJ. Further, DCF's employees, subcontractors, agents, or other affiliated third party persons or entities, as well as contracted third parties, must meet the same requirements of DCF under this Agreement and all amendments thereto with the DCF's employees, subcontractors, agents, contractors or other affiliated persons or entities and shall incorporate the terms and conditions of this Agreement into any contractual relationships currently existing or existing in the future.

1. Access Controls:
    a. Viewing and modification of Covered Data must be restricted to authorized individuals as required for business related use.
    b. Unique authorization is required for each person permitted access to Covered Data and access must be properly authenticated and recorded for audit purposes, including HIPAA, Payment Card Industry (PCI), and Criminal Justice Information Services (CJIS) audit requirements.
    c. Access to all Covered Data provided to DCF's employees, subcontractors, contractors, agents, or other affiliated persons or entities must meet the same requirements of the DCF under this Agreement and all amendments thereto with same and shall incorporate the terms and conditions of data security in the access authorization.
    d. User access to Covered Data must be disabled within twenty-four (24) hours after termination from employment or other change in employment where access to this data is no longer needed. User access must also be disabled after forty-five (45) days of inactivity.

2. Copying/Printing (applies to both paper and electronic forms):
    a. Covered Data should only be printed when there is a legitimate need.
    b. Access to copies must be limited to individuals authorized to access the Covered Data.
    c. Covered Data must not be left unattended.
    d. When copies of the Covered Data are no longer needed, they will be securely destroyed.

3. Network Security:
   a. All electronic communication including, but not limited to, Covered Data between DCF and DJJ shall use compatible, industry standard Secure File Transfer Protocol software, using data encryption or a Virtual Private Network connection to ensure a secure file transfer.
   b. Covered Data must be protected with a network firewall with "default deny" rule set required.
   c. Servers hosting the Covered Data cannot be visible to the entire Internet, nor to unprotected subnets.

4. Physical Security (servers, laptops and remote devices on which Covered Data is stored). For purposes of these standards, mobile devices must be interpreted broadly to incorporate current and future devices, which may contain or collect Covered Data:
   a. The computing device must be locked or logged out when unattended.
   b. Servers must be hosted in a secure data center hardened according to relevant security standards, industry best practices, and Department security policies.
   c. Physical access to servers containing Covered Data must ensure physical access is monitored, logged, and limited to authorized individuals at all times.
   d. Routine back-up of Covered Data is required and must be stored in a secure off-site location.

5. Remote access to systems hosting Covered Data:
   a. Remote access to Covered Data must be restricted to the local network or a secure virtual private network.
   b. Unauthorized remote access to Covered Data by third parties is not allowed.
   c. Access to Covered Data by all third parties must adhere to the requirements of this Agreement.

6. Data Storage:
   a. Storage of Covered Data on a secure server in a secure data center according to relevant security standards, industry best practices, and Department security policies is required.
   b. Covered Data stored on individual workstations or mobile devices must use full disk encryption with passwords. All mobile devices within the environment must have full disk encryption. If Covered Data is kept on the mobile device, any media, including flash cards, memory sticks, or external hard drives must be encrypted and stored in a secure location when not in use.
   c. Covered Data is not to be transmitted through e-mail or social networking sites unless encrypted and secured with a digital signature.
   d. Each Party will comply with the requirements of section 501.171,

Florida Statutes, regarding a breach of data containing personal information.

7. Antivirus protection shall be utilized on all mobile devices, workstations, and servers to safeguard the confidentiality and integrity of Covered Data. At a minimum, antivirus signatures shall be updated daily with full disk scans performed every two weeks.

V. Costs

This is a non-monetary agreement. Each agency will bear its respective cost for the data exchange and data match.

VI. Duration and Designation of Agreement Coordinators

A. This Agreement shall become effective on the last date of signature by the Parties and will terminate three (3) years from said date, unless renewed or terminated. This Agreement may be renewed for two consecutive one-year terms. An Annual Affirmation Statement (attached as Exhibit B) must be completed annually by DJJ by the Agreement anniversary date.

B. This Agreement may be renewed in writing with appropriate modifications as agreed upon by the Parties.

C. This Agreement replaces and incorporates all prior negotiations, interpretations, and understandings between the Parties. The Agreement may be mutually terminated by written agreement of the parties or unilaterally by either party, without cause, provided the terminating party serves the other party's Agreement Coordinator with written notice of an intent to terminate the Agreement in no less than thirty (30) days from the date such notice is sent. Either Party may terminate this Agreement for cause, without prior notice or warning, effective immediately upon written notice.

D. The Agreement Coordinators for this Agreement are:

DCF's IT Coordinator:
Kit Goodner, ACCESS Florida
1940 Monroe Street, Suite 80
Tallahassee, FL 32399
Kit.Goodner@myflfamilies.com
(850) 320-9191

DCF's Agreement Coordinator:
Janice "JD" Johnson
1317 Winewood Blvd., Bldg. 3, Rm. 454
Tallahassee, FL 32399-0700
JD.Johnson@myflfamilies.com
(850) 717-4110

DJJ's IT Coordinator:
Scott Morgan
2737 Centerview Drive
Tallahassee, FL, 32399
Scott.Morgan@djj.state.fl.us
(850) 717-2315

DJJ's Agreement Coordinator:
Mark Greenwald
2737 Centerview Drive
Tallahassee, FL 32399
Mark.Greenwald@djj.state.fl.us
(850) 717-2627

VII. Amendments and Changes

A. With the exception of changes to Agreement Coordinator designations (Section VI.D.) any changes, alterations, deletions, or additions to the terms set forth in this Agreement must be by written amendment executed by all Parties. Changes to Section IV.A. shall be accomplished as provided therein, changes to Section VI.D. may be accomplished by providing email change notification that is acknowledged by both Parties.

B. The Parties agree to follow and be bound by the terms and conditions of any policy decisions or directives from the federal and state agencies with jurisdiction over the use of the data contained herein upon receipt of written notice directing that such rules, policy decisions, or directives apply to this Agreement.

VIII. Inspection of Records

DCF shall permit DJJ or other state and federal representatives, or their designees, to conduct inspections described in this paragraph, or to make on-site inspections of records relevant to this Agreement to ensure compliance with any state and federal law, regulation, or rule. Such inspections may take place with notice during normal business hours wherever the records are maintained. DCF shall ensure a system is maintained that is sufficient to permit an audit of DCF's compliance with this Agreement and the requirements specified above. Failure to allow such inspections constitutes a material breach of this Agreement.

IX. Liability

It is understood that neither party to this Agreement is the agent of the other and neither is liable for the wrongful acts or negligence of the other. Each party shall be responsible for its negligent acts or omissions and those of its officers, employees, or agents, whosoever caused, to the extent allowed by law and without waiving the limits of sovereign immunity.

Florida Department Of Children and Families

Office of General Counsel

Signature

Kelly McGrath, Deputy General Counsel

3/20/15

Date

Program Office

Signature

Nathan Lewis, Director
Economic Self- Sufficiency

3.2015

Date

Chief Information Officer

Signature

Scott Stewart, Chief Information Officer

3/25/2015

Date

Department of Juvenile Justice

Chief of Staff

Signature

Fred Schuknecht, Chief of Staff

3/6/15

Date

Research and Planning

Signature

Mark Greenwald,

3-3-2015

Date

Chief Information Officer

Signature

Scott Morgan, Chief Information Officer

3/6/2015

Date

Exhibit A

DATA ELEMENTS

The list of data file will consist of the following:

First Name
Middle Name
Last Name
Date of Birth
Sex
Social Security Number
Admission Date
Actual Release Date (blank if youth is still in program)

Each resident must have been at the facility for 30 days or more in order to be included in the file. The file will be sent on a monthly basis, prior to the 10th of each month. All youth released since the last file was sent will be included in the file, as well, with actual release dates populated.

Exhibit B

Department of Children and Families
Annual Affirmation Statement

Agreement ID: _____ Date: _____

In accordance with Section VI., Part C, of the Data Sharing Agreement between the Department of Children and Families (Department) and Department of Juvenile Justice, the Department of Juvenile Justice hereby affirms that the Department of Juvenile Justice has evaluated and have adequate controls in place to protect the Covered Data from unauthorized access, distribution, use and modification or disclosure and is in full compliance as required in the Agreement between the Department and the Department of Juvenile Justice.

_____
Signature

_____
Printed Name

_____
Title

_____
Date

_____
Name of Agency