Attachment J
Contract Number:

DATA RELEASE AGREEMENT FOR RESIDENTIAL CHILD CARE AND CHILD PLACEMENT AGENCIES

I. PARTIES

This Agreement is between the Maryland State Department of Human Services (Social Services Administration and the Office of Licensing and Monitoring, hereinafter "DHS"), and the Residential Child Care Providers and the Child Placement Agency Providers (hereinafter "Organization"), collectively referred to as the "Parties".

____
NAME OF THE ORGANIZATION

II. PURPOSE

The purpose of this Agreement is to set forth the responsibilities of each of the Parties while serving DHS' clients under a contract or other agreement with DHS, which includes the completion and submission of services information, CANS assessment, uniform incident reporting (UIR), and service collaboration through the web-based *myDHR (or successor)* and CJAMS information systems. In addition, this Agreement sets forth the responsibilities of the Organization's users when accessing and using *myDHR (access should be requested using Sailpoint)* and CJAMS information systems (hereinafter "DHS Systems").

III. INTRODUCTION

Federal and state laws allow for the use and disclosure of information concerning children receiving foster care services, but place restrictions on the release of any information regarding the children served. The legal authority for use and disclosure of information is found in: 42 U.S. C. § 602(a)(1)(A)(iv); 42 U.S.C. § 1396a (a)(7); 7 C.F.R. § 272.1(c)(1); 42 C.F.R. § 431.300; 45 C.F.R. Part 160; 45 C.F.R. Part 164; 45 C.F.R. § 205.50; Md. Code Ann., Human Services § 1-201; and COMAR 07.01.07.

IV. RESPONSIBILITIES OF DHS

1. DHS shall designate a principal person and an alternate as the Point of Contact for the purpose of this Agreement.

2. DHS shall review a request for access to DHS Systems from the Organization for its staff member(s).

3. Once approved, DHS will certify that the Organization’s staff member(s) may enter the DHS Systems data for child(ren) in its care as required.

4. DHS shall assist in setting up the Organization’s staff member(s) with logon access, and will provide instructions for identified staff members when ready to begin use of DHS Systems.

5. Contractors (outside organizations) that will need access to CJAMS should use VPN that is provided by the DHS to access DHS environment.

V. RESPONSIBILITIES OF THE ORGANIZATION

1. The Organization must request that it be granted access to DHS Systems.

2. The Organization must submit a letter to the designated DHS security monitor requesting access to the DHS Systems for its staff member(s).

3. The Organization agrees that all information disclosed through this

Agreement is confidential and cannot be disclosed to any other person without written consent of DHS.

4. The Organization agrees that use of confidential information for purposes other than those authorized by DHS is strictly prohibited by state and federal law.

5. The Organization shall ensure that its agents, employees, and other designated persons agree to all provisions of this Agreement and will require all individuals who will have access to confidential information to execute a Non-Disclosure Agreement before they log into DHS Systems.

6. The Organization must instruct all persons having access to confidential information about the security requirements and that they are bound by the confidentiality provisions of this Agreement. The Organization must inform DHS immediately if an employee, or other designee who has access to DHS Systems has severed or been severed from any relationship with the Organization or has left employment, or if access is revoked for any reason.

7. The Organization must designate and provide DHS with the name and contact information for the individual who will serve as the administrative account manager responsible for providing and terminating DHS Systems account roles for its employees.

8. The Organization must immediately notify the DHS point of contact via email when the DHS Systems administrative account manager is no longer employed in that role.

9. The Organization must provide DHS with a list of all agents, employees and

other designated persons who have been given access to DHS Systems. This list must be kept current.

10. The Organization shall have sufficient process, protections and procedures in place to protect the data in accordance with State and federal law, and including the following:

a. Password protecting workstation with a “screensaver” password, set to automatically lock the system after a period of inactivity.

b. Computers must automatically lock after periods of inactivity. The period of inactivity prior to locking will be no greater than 15 minutes for devices containing DHS data.

c. Logging out of DHS Systems when workstations are left unattended.

d. Selecting a “strong” set of passwords and using different passwords for access to different systems.

e. A strong Passwords shall contain a combination of alphabetic uppercase and lower case, numeric, and special characters. Also, should be 14 characters at least.

f. Ensuring each device has an up-to-date virus protection installed that is maintained and patched daily.

g. Windows 10Professional 64-bit (or later versions supported by Microsoft) and the most current versions of Microsoft Edge or Google Chrome, with all current security patches and ongoing monthly patches for operating systems and applications.

h. USB ports must be protected such that no non-FIPS (Federal Information Processing Standards) compliant hardware level encryption devices that can store data can connect to the laptop, desktop or tablet.

i. Laptops must have Microsoft Defender or another endpoint security that can be used to track, freeze, and remotely wipe the device.

j. Portable Media Devices, including laptops, must have FIPS 140-2 Compliant hardware level encryption.

11. The Organization staff shall call the DHS OTHS Helpdesk at (410)767-7002 within one (1) hour when a security incident(s) involving the acquisition, access, use or disclosure of confidential information is suspected or detected so DHS may take steps to determine whether its system has been compromised and to take appropriate security precautions.

12. The Organization may not assign its rights or interests, nor delegate its duties under this Agreement, in whole or in part, without the express prior written consent of DHS. Any attempted assignment or delegation without such express prior written consent shall be void and ineffective for all purposes.

13. The Organization shall operate under this Agreement so that no person, otherwise qualified, is denied employment or other benefits on the grounds of race, color, sex, creed, national origin, age, marital status, sexual orientation, or physical or mental disability which would not reasonably preclude the required performance.

VI. **CONFIDENTIALITY**

DHS and the Organization shall protect the confidentiality of information obtained or accessed in the implementation of this Agreement. The use of the confidential information is confined to activities that are essential for the purpose of this Agreement.

VII. GENERAL PROVISIONS

1. Upon finding any breach of this Agreement by the Organization, DHS shall deny the use or access of DHS Systems to the Organization's staff members who violate this Agreement.

2. If the Organization no longer has a license to provide RCC/CPA services with OLM (Office of Licensing and Monitoring), this Agreement will be terminated.

3. If the Organization no longer provides RCC/CPA services under the contract with DHS but continues to have a license with OLM, this Agreement will continue.

4. The Organization may not use the confidential information for any purpose other than serving the children who have been placed in their programs, and their families.

5. The Organization agrees to hold the State of Maryland, DHS and its employees and officials harmless for loss, damages, and cost for any liability as a result of the disclosure or use of confidential information accessed or obtained during the administration and implementation of this Agreement.

6. The State of Maryland or DHS is not responsible for any loss or expenses that may be incurred by the Organization, its agents or employees as a result of an inability to access the DHS Systems.

VIII. TERM

1. The term of this Agreement will commence on October 1, 2025 and end September 30, 2028 . The Contract also contains one two-year renewal option. If the Contract is extended, this Data Sharing will also be extended.

2. Either Party may terminate this Agreement at any time following thirty (30) days written notice to the other Party.

IX. GOVERNING LAW

This Agreement and its construction, interpretation, and enforcement shall be construed in accordance with and governed by the laws of the State of Maryland.

X. CONTACT PERSONS

All notices, inquiries, or matters arising related to this Agreement, unless otherwise indicated in the Agreement, shall be between the points below. Each Party shall notify the other Party, in writing, of any changes to the points of contact. The point of contact for User Security and DHS Systems at the Department of Human

Services is:

Name: OTHS Service Desk

Division: Office of Technology for the Human Services

Address: Department of Human Services
Office of Technology for the Human Services
25 South Charles St.
Baltimore, Maryland 21201

Phone Number: (410) 767-7002

Email Address: Oths.helpdesk@maryland.gov

The point of contact person at SSA for DHS Systems in the Department of Human Services is:

Name: William Willoughby

Division: Social Services Administration

Address: Department of Human Services
Social Services Administration
25 South Charles St
Baltimore, Maryland 21201

Phone Number: 410-767-7277

Email Address: William.Willoughby@maryland.gov

The alternate point of contact person for the Department of Human Services is:

Name: Shernelle Crawford

Division: OTHS Chief Information Officer

Address: Department of Human Services
Office of Technology for the Human Services
25 South Charles St.
Baltimore, Maryland 21201

Phone Number: 410-238-1282

Email Address: shernelle.crawford@maryland.gov

The point of contact person for the Organization:

Name: ________________________

Organization: ________________________
Address: ________________________

Phone Number: ______________________

Fax Number: ______________________

Email Address: ______________________

Name: ______________________________________

Organization: ___________________________________
Address: ______________________________________

Phone Number:____________________________________

Email Address:____________________________________

SIGNATURE PAGE

IN WITNESS WHEREOF, intending to be legally bound, the Parties have caused this Agreement to be executed as of the dates indicated below.

DEPARTMENT OF HUMAN SERVICES

______________________________________ ______________________________

Name: Dr. Alger M. Studstill Jr. **Date Signed**
Title: Executive Director
Social Services Administration

____

NAME OF THE ORGANIZATION

______________________________________ ______________________________

Name: **Date Signed**

Title: __________________________________

APPROVED FOR FORM AND LEGAL SUFFICIENCY BY THE OFFICE OF THE ATTORNEY GENERAL