INTERGOVERNMENTAL AGREEMENT
BETWEEN
THE DEPARTMENT OF HUMAN SERVICES
AND
ILLINOIS STATE BOARD OF EDUCATION
2022-130-IGA-FCS

The Illinois Department of Human Services (DHS) and Illinois State Board of Education (ISBE) pursuant to the Intergovernmental Cooperation Act, 5 ILCS 220/1 *et seq.*, and the intergovernmental cooperation provisions of the Illinois Constitution, Ill. Const., Art. VII, Sec. 10, hereby enter into this Intergovernmental Agreement (Agreement) in connection with Child Find responsibilities, data transfer, and steps to ensure a smooth and effective transition (as specified below). DHS and ISBE are collectively referred to herein as the "Parties" and each, a "Party." To fulfill the terms of this Agreement the Parties agree to the following:

ARTICLE I
INTRODUCTION

1.1 Background. Infants and toddlers with disabilities (birth to age 3) and their families receive early intervention (EI) services under the Individuals with Disabilities Education Act, 20 U.S.C. § 1400 *et seq.*, as amended by the Individuals with Disabilities Education Improvement Act of 2004 (IDEA) Part C. Children (ages 3 to 22) receive special education and related services under IDEA Part B. DHS serves as the lead agency for Part C of IDEA. ISBE serves as the lead agency for Part B of IDEA.

1.2 Shared Child Find Responsibilities. DHS and ISBE both have Child Find responsibilities as defined under the IDEA 20 U.S.C. §§ 1412(a)(3) and 1435(a)(5), and 34 C.F.R. §§ 300.115, 303.302, and 303.303.

1.3 Notification Requirements. Not fewer than 90 days before the child's third birthday, DHS must notify ISBE and the Local Educational Agency (LEA) where the toddler receiving services resides that a toddler who is receiving Part C services and who is potentially eligible for services under the Part B section 619 preschool program will shortly turn 3 years old and exit the Part C program, in compliance with 34 C.F.R. § 303.209(b) & 34 C.F.R § 303.211(2)(i) and in alignment with 325 ILCS 20/11 Illinois Early Intervention Services System Act for eligible children to be offered extended Part C services until the start of the school year following their third birthday.

1.4 Purpose. This Agreement, among other things, specifies responsibilities to ensure a seamless transition of services under Part C and Part B of IDEA and to ensure the transfer of data from DHS to ISBE for transition and for ISBE's Annual Performance Report purposes. Federal regulations require DHS to have a transition interagency agreement.

ARTICLE II
DUTIES AND OBLIGATIONS OF THE PARTIES

2.1 Child Find and Public Awareness.

2.1.1 **Coordination of Child Find and Public Awareness.** ISBE acknowledges joint responsibility with DHS for Part C Child Find. ISBE shall continue to inform LEAs that they have

responsibilities under Part C, that they are the primary referral sources, and that they shall participate in Local Interagency Councils, in Child Find, and in public awareness activities, to the extent permitted by State and federal law, as set forth more fully below:

2.1.1.1 Public Awareness. ISBE shall require LEAs to conduct public awareness activities targeting families and other primary referral sources;

2.1.1.2 Screenings. ISBE shall require LEAs to conduct or arrange for screenings (by developmental checklists) to actively seek out infants and toddlers with disabilities or delays, report to DHS on these screenings, and maintain procedures to assure compliance with the five-day referral time frame (Schedules of screening dates and locations will be provided to the regional intake entity, other providers, and the local advisory body.);

2.1.1.3 Regional Intake Entities. ISBE shall require that LEAs work closely with their regional intake entity to assure evaluations of identified children; and

2.1.1.4 Local Advisory Body. ISBE shall require active participation in the local advisory body and as a member participate in coordination of public awareness and Child Find.

2.1.2 **Technical Assistance for Screening and Identification**. ISBE will provide technical assistance to LEAs to carry out screening and identification.

2.1.3 **Child Find Monitoring**. ISBE will monitor LEAs to assure that Child Find services are available in each LEA jurisdiction.

2.2 Data Access, Use and Security

2.2.1 Each Party certifies that it has the capacity to restrict access to the subject Data and maintain the security of electronic information, as for fully set forth in Appendix E (Data Security Plan). Each Party shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Data under the Agreement. These measures will be extended by contract to all employees, contractors, subcontractors, or agents that will receive Data provided by this Agreement and used by a Party.

2.3 EI Data Transfer for Transition.

2.3.1 **Transition Notification.**
For a toddler with a disability in EI greater than 90 days prior to the child's third birthday and is potentially eligible for preschool services under Part B, DHS will notify ISBE not fewer than 90 days before the child's third birthday that the toddler on his or her birthday will reach the age of eligibility for services under Part B. DHS shall allow disclosure to ISBE of personally identifiable information and contact information regarding Part C EI clients for the purpose of transition and Child Find as required by law. These clients may be

eligible for preschool services under Part B and could transition from receiving early intervention services under Part C to potentially receiving special education and related services under Part B.

For a toddler who is determined eligible for EI services more than 45 days but less than 90 days before the toddler's third birthday, transition notification will be provided as soon as possible after determining the toddler's eligibility.

If a child is referred to the regional intake entity, also known as the Child and Family Connections office (CFC), fewer than 45 days before the toddler's third birthday, the referral information will be sent (with parental consent) by the regional intake entity to the LEA and to the early intervention program, which will forward the information to ISBE.

The identifying information to be disclosed includes only the child's name, date of birth, and parent/guardian contact information (including parent/guardians' names, addresses, telephone numbers and primary language) to ISBE. DHS and ISBE will protect the confidentiality of such information and comply with all applicable federal and State laws regarding confidentiality. This Agreement does not negate any DHS policies or procedures regarding consent during the transition process. However, consent is not required to disclose the above information as set forth herein.

2.3.2 **Use of Transition Notification Data**. ISBE will use the information disclosed for the purpose of monitoring transition and Child Find duties under IDEA. Any other use of the information disclosed is strictly prohibited, except with the prior written consent of DHS in an amendment to this Agreement.

2.3.3 **Transfer of Transition Notification Data to LEA**. Not fewer than 90 days prior to the child's third birthday, ISBE will forward the child's identifying information to the LEA where the toddler receiving Part C services resides.

2.4 Data Transfers.

2.4.1 **Data Transfer for Federal Reporting Requirements and Monitoring of Transition and Child Find Duties Under IDEA**. Data required for the U.S. Department of Education's Annual Performance Report will be provided to ISBE no later than November 1 of each year. Specifically, DHS will provide ISBE child-specific information, including termination reason and date for families who have consented to transition.

2.4.2 **Required Evaluation and Outcome Measurement**. DHS and ISBE will work cooperatively to share data for purposes of program evaluation and outcome measurement, as called for the in the Government and Performance Results Act of 1993, 5 U.S.C. § 306 and 31 U.S.C. § 1115 *et seq.*, as amended by the Government Performance and Results Modernization Act, within the confines of the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g), and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 300gg and 29 U.S.C. § 1181 *et seq.* and 42 U.S.C. 1320d *et seq.*, as amended. This Agreement shall be modified to accommodate that use of client data when the Parties agree that an acceptable process can be implemented.

2.5 Smooth and Effective Transition.

2.5.1 **Transition Plan.** DHS will require regional intake entities to hold Individualized Family Services Plan (IFSP) team meetings not fewer than 90 days and, at the discretion of all parties, not more than nine months before the toddler's third birthday for the IFSP team, including the family, to develop/update a transition plan to include steps for the toddler with a disability and his/her family to exit the EI program and any transition services that the IFSP team identifies as needed by that toddler and his/her family. The transition planning conference and the IFSP team meeting to develop the transition plan may be combined into one meeting.

The service coordinator should facilitate the IFSP team meeting during which the transition plan is established to ensure that program options for the toddler with a disability for the period from the toddler's third birthday through the remainder of the school year are reviewed and each family is included in the development of the transition plan. The transition plan in the IFSP should identify the steps for the toddler with a disability and his family to exit from the Part C program and any transition services that the IFSP team identifies as needed by that toddler and his or her family to support a smooth transition to preschool services under Part B to the extent that those services are appropriate of other appropriate services. The steps must include the following:

- Discussions with, and training of, parents/guardians (as appropriate) regarding future placements and other matters related to the child's transition;
- Procedures to prepare the child for changes in service delivery, including steps to help the child adjust to, and function in, a new setting;
- Confirmation that Child Find information about the child has been transmitted to the LEA or other relevant agency;
- Confirmation that, with parental consent, additional information needed by the LEA to ensure continuity of services from the Part C program to the Part B program has been sent to the LEA, including a copy of the most recent evaluation and assessment of the child and the family and most recent IFSP; and
- Identification of transition services and other activities that the IFSP team determines are necessary to support the transition of the child.

The transition planning conference and the IFSP team meeting to develop the transition plan may be combined into one meeting. The IFSP team meeting to develop the transition plan must be held in settings and at times that are convenient for the family and in the native language of the family or other mode of communication used by the family, unless it is clearly not feasible to do so. Meeting arrangements must be made and written notice provided to the family and other participants early enough before the meeting date to ensure that they will be able to attend. The contents of the IFSP must be fully explained to the parents/guardians and informed written consent obtained prior to the provision of the EI services described in the IFSP. Each EI service must be provided as soon as possible after the parent/guardian provides consent for that service.

The IFSP team meeting to develop the transition plan must include the following participants: the parent(s)/guardian(s) of the child, other family members as requested

by the parent/guardian if feasible to do so, an advocate or person outside the family if the family requests that person participates, the service coordinator, persons directly involved in conducting evaluations and assessments, and persons who will be providing EI services to the child or family. If a person or persons directly involved in conducting evaluations and assessments is unable to attend a meeting, arrangements must be made for the person's involvement through other means, including one of the following: participating in a telephone conference, virtually or having a knowledgeable equally qualified provider attend the meeting.

2.5.2 **Transition Conference**. DHS shall require the regional intake entity, if a toddler with a disability may be eligible for Part B preschool services and with the family's approval, to convene a transition conference with the appropriate parties to discuss any services the toddler may receive under Part B. The conference must be held no later than 90 days before the toddler's third birthday, but, at the discretion of all parties, may occur up to nine months before the toddler's third birthday.

The transition planning conference and the IFSP team meeting to develop the transition plan may be combined into one meeting. The IFSP team meeting to develop the transition planning conference must be held in settings and at times that are convenient for the family and in the native language of the family or other mode of communication used by the family, unless it is clearly not feasible to do so. Meeting arrangements must be made and written notice provided to the family and other participants early enough before the meeting date to ensure that they will be able to attend. The contents of the IFSP must be fully explained to the parents/guardians and informed written consent obtained prior to the provision of the EI services described in the IFSP. Each EI service must be provided as soon as possible after the parent/guardian provides consent for that service.

In addition to the LEA, the transition planning conference must include the following participants: the parent(s)/guardian(s) of the child, other family members as requested by the parent/guardian if feasible to do so, an advocate or person outside the family if the family requests that person participates, the service coordinator, a person or persons directly involved in conducting evaluations and assessments, and as appropriate, persons who will be providing EI services to the child or family. If a person or persons directly involved in conducting evaluations and assessments is unable to attend a meeting, arrangements must be made for the person's involvement through other means, including one of the following: participating in a telephone conference, virtually or making pertinent records available at the meeting (i.e., providing, with parental consent, the most recent evaluation(s) and/or assessment(s) of the child, if not already provided in the referral packet). If a person or persons directly involved in conducting evaluations and assessments is unable to attend the transition planning conference, attempts to secure his/her attendance should be documented in case notes.

2.5.3 **LEA Communication**. ISBE shall require the LEA to communicate with the service coordinator on any activities related to transitioning to Part B services.

2.5.4 **Participation in Transition Conferences**. ISBE shall require the LEA to participate in transition conferences arranged by the EI regional intake entity for toddlers with disabilities who may be eligible for preschool services under Part B.

2.5.5 **Implementation of Individualized Education Program (IEP) and Individualized Family Services Plan (IFSP)**. ISBE shall ensure that an IEP, or if consistent with IDEA sections 614(d)(2)(B) and 636(d), an IFSP, has been developed and is being implemented by the child's third birthday.

2.5.6 **Invitation to IEP Meeting**. At the request of the parent/guardian, ISBE shall require the LEA to send an invitation to the initial IEP meeting to the Part C service coordinator, or other Part C service representative, if the child previously received Part C services.

2.5.7 **Consideration of IFSP by IEP Team**. For all children who transition from Part C services to Part B, ISBE shall require the IEP team to consider an IFSP that contains the IFSP content (including the natural environments statement) described in IDEA section 636(d) and its implementing regulation when developing the initial IEP.

2.5.8 **Part B Services**. ISBE shall ensure that for those children transitioning from Part C to Part B, who are determined to be eligible for services through Part B, that LEAs provide appropriate services to them, including extended school year services, and shall do so pursuant to IEPs developed for such children in accordance with 34 C.F.R. §300.309 as further provided by 23 Ill. Admin. Code 226.260(a) and (c) and 226.750(c).

2.6 Participation on the Illinois Interagency Council on Early Intervention (IICEI). ISBE shall designate Early Childhood Special Education or Special Education management personnel or their designee who has sufficient authority to engage in policy planning and implementation on behalf of ISBE as its representative to the IICEI. The staff person so designated shall attend and fully participate in IICEI meetings, or if not available on a meeting date and time, designate another such staff person with such authority to attend and fully participate.

2.7 Contacts for Compliance.

2.7.1 **LEA Compliance**. If notified by DHS that an LEA is not providing appropriate public awareness, Child Find, or transitioning as set forth below, ISBE will contact the LEA to ensure the establishment of appropriate awareness, screening, identification, and transitioning.

2.7.2 **Provider Compliance**. If notified by ISBE that a credentialed or enrolled provider is not cooperating appropriately with LEAs with regard to Child Find, public awareness or transition activities, DHS will contact the provider to require appropriate cooperation.

2.8 EI Monitor Responsibilities. DHS shall comply with monitoring responsibilities as set forth in 34 C.F.R. §303.209. With regard to Child Find, public awareness and transition activities, DHS, to the extent permitted by state and federal law, shall monitor contractual and enrolled providers of EI services as set forth in 89 Ill. Admin. Code 500.65.

ARTICLE III
TERM

3.1 Term. This Agreement shall commence upon execution, and, unless otherwise terminated by the Parties, shall continue through June 30, 2025. In no event will the total term of the Agreement, including the initial term, any renewal terms and any extensions, exceed 10 years.

ARTICLE IV
TERMINATION

4.1 (a) This Agreement may be terminated by either Party for any or no reason upon thirty (30) days' prior written notice to the other Party.

(b) Either Party may terminate this agreement, in whole or in part, for cause immediately upon notice to the other Party if: (i) a Party determines that the actions or inactions of the other Party, its agents, employees or subcontractors have caused, or reasonably could cause, jeopardy to health, safety, or property, or (ii) a Party has notified the Party claiming breach that it is unable or unwilling to perform the agreement.

In the event either Party breaches this Agreement by failure to perform to the other Party's satisfaction any material requirement of this Agreement or is otherwise in violation of a material provision of this Agreement and fails to cure such breach within ten (10) days' written notice thereof from the Party claiming breach, the Party claiming breach may terminate this Agreement upon written notice to the breaching Party.

For termination due to any of the causes contained in this Section, each Party retains its rights to seek any available legal or equitable remedies and damages.

ARTICLE V
MISCELLANEOUS

5.1 Renewal. This Agreement may be renewed for additional periods by mutual consent of the Parties, expressed in writing and signed by the Parties.

5.2 Amendments. This Agreement may be modified or amended at any time during its term by mutual consent of the Parties, expressed in writing and signed by the Parties.

5.3 Applicable Law and Severability. This Agreement shall be governed in all respects by the laws of the State of Illinois. If any provision of this Agreement shall be held or deemed to be or shall in fact be invalid, inoperative or unenforceable as applied in any particular case in any jurisdiction or jurisdictions or in all cases because it conflicts with any other provision or provisions hereof or any constitution, statute, ordinance, rule of law or public policy, or for any reason, such circumstance shall not have the effect of rendering any other provision or provisions contained herein invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of any one

or more phrases, sentences, clauses, or sections contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof. In the event that this Agreement is determined to be invalid by a court of competent jurisdiction, it shall be terminated immediately.

5.4 Records Retention. The Parties shall maintain adequate books, records, and supporting documents to comply with 89 Ill. Admin. Code 509 for a minimum of five (5) years from the later of the date of final payment under this Agreement or the expiration of this Agreement. If an audit, litigation, or other action involving the records is begun before the end of the five-year period, the records shall be retained until all issues arising out of the action are resolved.

5.5 No Personal Liability. No member, official, director, employee, or agent of either Party shall be individually or personally liable in connection with this Agreement.

5.6 Disclaimer. ISBE shall not be held liable for any improper or incorrect use of the Data by an LEA and assumes no responsibility for or relating to the integrity, privacy, security, confidentiality, or use of the Data by an LEA.

5.7 Assignment; Binding Effect. This Agreement, or any portion thereof, shall not be assigned by any of the Parties without the prior written consent of the other Parties. This Agreement shall inure to the benefit of and shall be binding upon the Parties and their respective successors and permitted assigns.

5.8 Precedence. In the event there is a conflict between this Agreement and any of the attachments hereto, this Agreement shall control. In the event there is a conflict between this Agreement and relevant statute(s) or Administrative Rule(s), the relevant statute(s) or rule(s) shall control.

5.9 Entire Agreement. This Agreement constitutes the entire agreement between the Parties; no promises, terms, or conditions not recited, incorporated, or referenced herein, including prior agreements or oral discussions, shall be binding upon either Party.

5.10 Notices. All written notices, requests, and communications may be made via mail, fax, or electronic mail to the addresses set forth below.

To DHS:
Grace B. Hou
Secretary
Illinois Department of Human Services
100 South Grand Avenue East, 3rd Floor
Springfield, IL 62762
Grace.Hou@illinois.gov

To ISBE:
Dr. Carmen Ayala
State Superintendent of Education
Illinois State Board of Education
100 North 1st Street
Springfield, IL 62777

5.11 Availability of Appropriations. The Parties' respective obligations hereunder shall cease immediately, without penalty, if: (a) the Illinois General Assembly fails to make an appropriation sufficient to pay such obligations; (b) adequate funds are not appropriated or granted to the respective Parties by the Illinois General Assembly to allow the respective Parties to fulfill their obligations under this Agreement; or (c) funds appropriated are de-appropriated or not allocated.

5.12 Headings. Section and other headings contained in this Agreement are for reference purposes only and are not intended to describe, interpret, define, or limit the scope, extent, or intent of this Agreement or any provision hereof.

5.13 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be considered to be one and the same agreement, binding on all Parties hereto, notwithstanding that all Parties are not signatories to the same counterpart. Duplicated signatures, signatures transmitted via facsimile, or signatures contained in a Portable Document Format (PDF) document shall be deemed original for all purposes.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their duly authorized representatives on the dates shown below .

ILLINOIS STATE BOARD OF EDUCATION

Carmen Ayala

Dr. Carmen Ayala
State Superintendent of Education

Designee Signature

Printed Designee Name

Designee Title

08/23/2022

Date

ILLINOIS DEPARTMENT OF HUMAN SERVICES

Grace B. Hou by Kathyn Smith 4

Grace B. Hou
Secretary

Kathyn Smith

Designee Signature

Kathyn Smith

Printed Designee Name

Private Secretary II

Designee Title

January 3, 2022

Date

SECURITY ANNEX
INFORMATION SECURITY AND AUDIT COMPLIANCE

1.1. Security Requirements.
The User agrees to comply with the security requirements established by IDHS and Illinois Department of Innovation and Technology (DoIT). The User also agrees to use the Data solely for the authorized purposes in accordance with the terms of this Agreement.

a) The User shall comply with Illinois DoIT and IDHS IT security and privacy policies and guidelines. The following requirements are drawn from these documents:

- DoIT Enterprise Security Polices: https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx
- HIPAA Administrative Directives: http://intranet.dhs.illinois.gov/onenet/page.aspx?item=12670
- IDHS Management of Information Services (MIS) Standard, I170-10, Data Security Policy: http://intranet.dhs.illinois.gov/onenet/page.aspx?item=13959
- IDHS MIS Standard I170-60, Password Standards: http://intranet.dhs.illinois.gov/onenet/page.aspx?item=15278
- IDHS MIS Standard I170-80, Security/Integrity Breaches: http://intranet.dhs.illinois.gov/onenet/page.aspx?item=15282

b) The security requirements may be updated to address changes in processes or technologies, as well as new or revised federal security requirements and guidelines. In such instances, IDHS shall provide the User with written notification of such changes and the timeframe for compliance and require written assurance by the User that it shall comply with new or revised security requirements.

c) The security requirements with which the User shall comply as a condition of receiving information from the IDHS are presented in three categories: administrative, technical and physical, and three additional sections: Breach Reporting and Notification Responsibility, Security Certification and Audit Requirements.

1.2. General Information

a) Use must also complete the Data Elements and Transmission form, Appendix A of this Agreement.

b) The Data will only be stored in an appropriate manner as defined below.

c) Only one complete copy of the Data is permitted to be maintained by Recipient; however, time-delimited temporary data analysis files may be created. Any temporary data file(s) and subsets of the original data set will be considered Data and subject to the terms and conditions of this Agreement.

d) Protected Health Information (PHI), Individually Identifiable Health Information (IIHI), Personally Identifiable Information (PII), Social Security Numbers, and Federal Tax Information (FTI) may require additional security and privacy safeguards due to federal or state statutory requirements. The user must be familiar with their responsibilities to protect the confidentiality, integrity and availability of this Data per the below Statutory requirements:

i) Health Insurance Portability and Accountability (HIPAA), 45 CFR Part 160, Part 162, and Part 164
ii) The Privacy Act of 1974, 5 U.S.C. 552a
iii) IRS Publication 1075

1.3. Administrative Security Requirements

a) The User shall restrict access to, and disclosure of, the Data to only authorized personnel who need the Data to perform their official duties in connection with the authorized purposes specified in the agreement.

b) The User shall establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to the Data.

c) The User shall advise all authorized personnel who access the Data of the confidentiality of the Data, the safeguards required to protect the results, and the civil and criminal sanctions for noncompliance contained in the applicable federal and state laws, including Section 453(1)(2) of the Social Security Act. 42 U.S.C. § 653(1)(2).

d) The User shall deliver security awareness training for authorized personnel and maintain a copy of the training received. The training shall include information about the responsibility of such personnel for proper use and protection of the Data, and the possible sanctions for misuse. All personnel shall receive security awareness training prior to accessing the Data, and at least annually thereafter. Such training shall address the Privacy Act of 1974, other federal and state laws governing computer security and the use and misuse of PII information.

e) The User's personnel with authorized access to the Data shall sign IDHS External Certificate of Understanding and Confidentiality Agreement (see Appendix B) which outline the authorized purposes for which the Data may be used by the User and the civil and criminal penalties for unauthorized use.

f) The User shall maintain records of authorized personnel with access to the Data. The records shall contain a copy of each individual's signed Certificate of Understanding and Confidentiality Agreement and proof of the individual's participation in security awareness training. The User shall make such records available to IDHS within two working days of a request for such records. Such records are to be maintained for three (3) years.

g) The User shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving PHI/IIHI/PII as applicable), or suspected incidents involving the Data. The User shall report confirmed and suspected incidents in either electronic

or physical form to the IDHS Privacy Officer and the IDHS Chief Information Security Officer (CISO) designated on this security annex immediately upon discovery, but in no case later than one hour of discovery of the incident. The requirement for the User to report confirmed or suspected incidents involving the Data to IDHS exists in addition to, not in lieu of, any User requirements to report to any other reporting agencies.

1.4. Technical Security Requirements

a) Access via remote terminal/workstation over the Public Internet. Remote data access is prohibited unless Recipient requests remote access and Agencies authorize remote access as part of this Agreement. If requesting remote access the Recipient will include the safeguards in place to secure the receipt and transmission of Data.

b) Wireless Area Network (WAN) or wireless access points, if utilized by the User, must be secured in accordance with the current revision of NIST 800-53; NIST 800-153 provides guidelines for Securing Wireless Local Area Networks.

c) The User shall utilize and maintain technological (logical) access controls that limit access to Data to only those personnel identified in the records maintained by the User pursuant to Sections II.A.6 and II.C.2 of this security annex who are authorized for such access based on their official duties.

d) The User shall implement controls to authenticate, authorize, evaluate, and remediate wired, wireless and Vendor before a device may access the network. Solutions such as Network Access Control, a Network Admission Control (NAC) solution or commensurate security controls may be used to enforce security policy compliance on all devices that attempt to gain access to, or use, the Data. The solution chosen or employed must be capable of evaluating whether remote machines are compliant with security policies through host(s) integrity tests against redefied templates such as patch level, service packs, antivirus and personal firewall status, and custom-created checks tailored for the state enterprise environment. The solution enforces security policies by blocking, isolating or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit or report on Vendors' access and presence on the state network. If unable to implement a full NAC-like solution, the Vendor must employ security controls that provide assurance that remotely connected devices pose no risk to the system or data being accessed.

e) The User shall implement access control procedures and account management that provides an adequate level of security and privacy commiserate to the confidentiality and sensitivity of the data being shared.

f) The User transmits all Data provided pursuant to this agreement in a manner that safeguards the Data and prohibits unauthorized access. The User and IDHS exchange the Data via a mutually-approved and secured data transfer method which utilizes a FIPS 140-2 compliant, NIST-certified encryption solution (i.e. VPN) if encryption is required in cases of Social Security Number. If wireless access is utilized by the User facility, then it shall be FIPS 140-2 compliant if used to connect to IDHS.

1. PHI, IIHI, and Social Security Numbers must be encrypted as stated above when transmitted via e-mail.

g) The User shall prohibit the use of personally owned (e.g., personal computers, mobile devices such as Blackberries, iPhones, IPODs, MP3 players, USB/Flash drives, external hard drives, CD/DVDs) and other non-agency furnished equipment used to connect to and access Data locally or remotely unless specifically requested by the User and authorized within this Agreement.

h) Data Storage

1. The User shall prohibit the Data from being copied to and stored at User site(s) on mobile media (e.g., laptops, CD-ROMs, USB drives) unless specifically requested by the Recipient and authorized within this Agreement.

2. Data shall not be stored by Recipient on portable devices or media which include but are not limited to laptops, tablets, handhelds/PDAs, Ultramobile PCs, optical discs, CDs, DVDs, Blu-Rays, removable storage and flash memory devices unless specifically requested by the Recipient and authorized within this Agreement. The request must include methods for encrypting the Data, controlling access to the data and physically protecting the device(s) containing the Data.

3. User agrees to store Data on one or more of the following media and protect the Data as described:

(i) Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized Users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

(ii) If the workstation is located in an unsecured physical location the hard drive must have encryption to protect the Data in the event the device is stolen.

(iii) Data stored on hard disks mounted on network servers and made available through shared folders.

(iv) Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

(v) Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

(vi) Backup copies for DR purposes must be encrypted if recorded to removable media.

i) Data Segregation

(i) Data must be segregated or otherwise distinguishable from non-sensitive data or information. This is to ensure that when no longer needed by the Recipient, all Data can be identified for return or destruction. It also aids in determining whether Data has or may have been compromised in the event of a security breach.

1. Data shall be stored in one of the following methods:

(i) Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non- sensitive data; or

(ii) Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to such data; or,

(iii) Data will be stored in a database which will contain no non-sensitive data; or,

(iv) Data will be stored within a database and will be distinguishable from non- sensitive data by the value of a specific field or fields within database records; or

(v) When it is not feasible or practical to segregate Data from non-sensitive data, then both the Data and the non-sensitive data with which it is commingled must be protected as described in this Agreement.

1.5. Physical Security Requirements

a) All Data shall be stored in a secure environment physically located in the continental United States with access limited to the least number of staff needed to complete the purpose of this Agreement.

b) User equipment containing IDHS data (servers, routers, hubs, etc.) are to be maintained in secure spaces or those off limits to the general public where access is restricted to authorized employees or contractors, vendors and delivery personnel who have a business purpose for being there.

c) Individuals who are not employees or contractors of User may not be present in these spaces unless escorted by authorized User personnel.

d) Users shall not leave workstations unattended while accessing IDHS data. If the employee leaves their workstation, they must lock (Ctrl-Alt-Del function) their computer so as not to expose IDHS PII to unauthorized personnel/passersby.

e) Paper documents containing PHI/IIHI/PII as applicable must be stored securely in locked offices, rooms, cabinets and/or desks.

1. Disposal of Paper Documents and Electronic Media Containing PHI/IIHI/PII as applicable

(i) Upon termination of the Agreement, User shall dispose of IDHS PHI/IIHI/PII as applicable received along with backup copies and any temporary or permanent work files that contain Data and provide written notification of disposal. Disposal must be in accordance with NIST 800-53 r4. Failure to do so may prevent data sharing agreements with the organization in the future.

(ii) Upon the destruction of the Data, the Recipient shall complete Appendix C of this Agreement, Certification of Data Disposition, and submit it to Agencies' authorized representatives within fifteen (15) days of the date of disposal.

(iii) Paper documents that contain PHI/IIHI/PII as applicable must be shredded for disposal and is prohibited from being disposed in the office trash. A contract with a recycling firm to recycle sensitive or confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

(iv) If data has been stored on server or workstation data hard drives, removable media (e.g. floppies, USB Flash Drives, portable hard disks, etc) or similar media, the data User shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

2. Acceptable destruction methods for various types of media include:

(i) For paper documents containing sensitive or confidential information, a contract with a recycling firm to recycle sensitive or confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

(ii) For paper documents containing data requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.

(iii) If data has been contained on optical discs (e.g. CDs, DVDs, Blu-ray), the data User shall either destroy by incineration the disc(s), shredding the discs, or completely deface the readable surface with a coarse abrasive.

(iv) If data has been stored on magnetic tape(s), the data User shall destroy the data by degaussing, incinerating or crosscut shredding.

(v) If data has been stored on server or workstation data hard drives or similar media, the data User shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

(vi) If data has been stored on removable media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

1.6. Incident Handling And Notification Responsibility

a) Upon disclosure of information from IDHS to the User, the User is the responsible party in the event of a breach or suspected breach of the information. Within one hour of discovery of the breach or suspected breach, the User is responsible for reporting the breach or suspected breach to the IDHS security officials listed in this 5.8, Person's to Contact.

b) The User is responsible for all reporting and notification activities, including but 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 the Data;
- performing any necessary follow-up activities to correct the vulnerability that allowed the breach;
- any other activities as required by IDHS.

c) Additional information regarding Security/Integrity Breaches can be found in IDHS MIS Standard I170-80, Security/Integrity Breaches: http://intranet.dhs.illinois.gov/onenet/page.aspx?item=15282

1.7. Security Certification

a) Security Posture

1. The User submits to the IDHS Chief Information Security Officer an IDHS Security and Privacy Controls Questionnaire, Appendix D, and any required documentation for approval prior to the sharing of IDHS data to ensure security and privacy control requirements are met.

b) Security And Privacy Self-Assessment And Certification Of Compliance

1. The User submits annually to IDHS an updated SPCQ that details the measures the User has in place to comply with the requirements specified in this security addendum. This SPCQ contains a certification of compliance that is signed by an authorized official of the User to certify that information provided in the SPCQ is accurate.

1.8. Audit Requirements

1. IDHS reserves the right to audit the User or make other provisions to ensure that the User is maintaining adequate safeguards to secure the Data. Audits ensure that the security policies, practices and procedures required by IDHS are in place within the User.

1.9. Persons To Contact

1. The IDHS HIPAA Chief Privacy Officer
   Patricia M. Brown
   100 W. Randolph St., Suite 6-400
   Chicago, IL 60601
   Phone: 312-814-2717
   Patricia.M.Brown@Illinois.gov

2. The IDHS Chief Information Security Officer:
   Kory Chapman
   Chief Information Security Officer,
   Bureau of Information Security and Audit Compliance
   Illinois Department of Human Services
   100 South Grand Avenue East
   Springfield, Illinois 62762
   Phone: 217-557-6614
   Kory.Chapman@Illinois.gov

APPENDIX A

DATA ELEMENTS AND TRANSMISSION

Check All that Apply:

IDHS Data is to be **SENT (pushed) TO** the User in one of the methods below: Yes [X] No [ ]

- [X] Electronic Transmission (i.e. SFTP/FTP, Cyberfusion, etc)
- [ ] Postal Mail: Paper
- [ ] Postal Mail: Electronic Media (i.e.CD/Flash/ect)

IDHS Data is to be **RECIEVED (pulled) FROM** the User in one of the methods below: Yes [ ] No [X]

- [ ] Electronic Transmission (i.e. SFTP/FTP, Cyberfusion, etc)
- [ ] Postal Mail: Paper
- [ ] Postal Mail: Electronic Media (i.e.CD/Flash/ect)

IDHS Data is to be **STORED** at the User's facility: Yes [X] No [ ]

IDHS Data is to be **PROCESSED and SENT BACK** to IDHS by User in one of the methods below:

Yes [ ] No [X]

- [ ] Electronic Transmission (i.e. SFTP/FTP, Cyberfusion, etc)
- [ ] Postal Mail: Paper
- [ ] Postal Mail: Electronic Media (i.e.CD/Flash/ect)

SPECIFIC DATA ELEMENTS

DATA ELEMENT	DATA CLASSIFICATION	ENCRYPTION	DATA SOURCE
Cornerstone Participant ID	Confidential		EI Data System
Name	Protected		EI Data System
Date of Birth	Protected		EI Data System
School District Code	Public		EI Data System
County Code	Public		EI Data System
Clinic ID	Confidential		EI Data System

Contact Name	Protected		EI Data System
Address	Protected		EI Data System
Phone Number	Protected		EI Data System
Early Intervention ID	Confidential		EI Data System
Primary Language	Protected		EI Data System

If additional rows are needed, please recreate above table and attach to agreement.

DATA CLASSIFICATION:

Public: Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to our clients, IDHS, the State of Illinois, our providers and partners. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Confidential: Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to our clients, IDHS, the State of Illinois, our providers and partners. By default, all IDHS Data that is not explicitly classified as Protected or Public data should be treated as Confidential data. A reasonable level of security controls should be applied to Confidential data.

Protected: Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to to our clients, IDHS, the State of Illinois, our providers and partners. Examples of Protected data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Protected data. This includes Personally Identifiable Information (PII), Personal Health Information (PHI), Individually Identifying Health Information (IIHI) and Federal Tax Information (FTI).

APPENDIX B

Certificate of Understanding and Confidentiality Agreement

IGA/DSA #_____

I understand that all information and data received from the Illinois Department of Human Services (IDHS) under the IGA/DSA listed above is confidential and must be protected from unauthorized use and disclosure.

I understand and agree that all such information or data (oral, visual or written, including both paper and electronic) which I see or to which I have access may not be released, copied or disclosed, in whole or in part, unless authorized by IDHS.

When I no longer require access to confidential information, whether because of termination of employment, reassignment of duties or otherwise, I agree that I will not access or attempt to access any IDHS confidential information, or any confidential information in IDHS systems or other sources to which I have been given access. I will return any and all reports, notes, memoranda, notebooks, drawings, and other confidential information or data developed, received, compiled by or delivered to me in order to carry out functions under the contract or subcontract, regardless of the source of the confidential information or data.

I understand that the law forbids releasing or disclosing such confidential information, in whole or part. I further understand that if I am unsure as to what information is confidential, I will immediately and prior to any such disclosure consult with IDHS or my supervisor.

I will safeguard, and will not disclose to unauthorized parties, any user name and/or password that may be issued to me in furtherance of my access to the confidential information. I understand that my access to the confidential data may be revoked at any time for any other reason at the discretion and direction of IDHS or my supervisor.

I will comply with all applicable Federal and State laws and regulations and with all applicable policies and procedures as set by the State of Illinois, including, but not limited to, the Illinois Public Aid Code

(305 ILCS 5/1 *et seq.*), the Health Insurance Portability and Accountability Act (45 CFR Parts 160, 162, and 164), IRS Code (26 U.S.C. 1 *et seq.*), and other applicable state and federal laws.

I will promptly report to my supervisor or IDHS Information Security and Audit Compliance Bureau any activities by any individual or entity that I suspect may compromise the availability, integrity, security or privacy of the confidential information. I will immediately notify my supervisor of any request for confidential information or data received from an individual or entity not authorized to receive the data under the IGA/DSA listed above.

I agree not to attach or load any additional hardware or software to or into IDHS equipment/applications unless authorized to do so. I will use only my access rights to, and will access only those systems, directories, confidential information or data authorized for my use by IDHS.

I agree to store confidential information received in secure, locked containers or, where data is stored on a computer or other electronic media, in accordance with IDHS' computer security policy that protects confidential information from unauthorized disclosure.

I understand and agree that the terms of this Confidentiality Agreement shall continue even when I am no longer employed by the agency which is covered by the IGA/DSA indicated above, and that I will abide by the terms of this Confidentiality Agreement in perpetuity.

I understand that failure to comply with these requirements may result in disciplinary action, termination, monetary penalties and criminal prosecution, as well as any other penalties provided by law.

This Agreement shall be governed by the laws of the State of Illinois, unless otherwise required by the Federal Supremacy Clause.

Signature Date

_____

Name (Printed)

APPENDIX C

Certification of Data Disposition

Date of Disposition _____

I hereby attest that with regards to the Data Share and Use Agreement between IDHS, and User that was executed on _____ [insert date of execution]

___ All copies of any data have been wiped from data storage systems.

___ All materials and non-wiped computer media containing any data sets have been destroyed.

___ All copies of any data that have not been disposed of in a manner described above, have been returned to Agencies' authorized representative as listed in this Agreement.

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in the above-captioned Data Share and Use Agreement, Security Annex, Section C, of this Agreement have been fulfilled as indicated above.

Signature of Recipient's Authorized Representative_____

Print Name of Recipient's Authorized Representative_____

Date: _____

APPENDIX D

The SPCQ is a questionnaire that serves to outline your Organization/Agency's baseline security and privacy controls as they relate to the Intergovernmental/ Data Agreement (IGA/DSA) contractual requirements to access the Illinois Department of Human Services (IDHS) and Healthcare and Family Services (HFS)data, documents and electronic media.

- The baseline control questions are in accordance with the Federal and State laws, policies and audit compliance regarding how IDHS/HFS provides security and privacy of our client's data and personal information.
- Link to the required Security Questionnaire: **https://www.dhs.state.il.us/page.aspx?item=88105**

EXHIBIT A - STANDARD CERTIFICATIONS FOR INTERGOVERNMENTAL AGREEMENTS

Public Agency acknowledges and agrees that compliance with this section and each subsection for the term of the contract and any renewals is a material requirement and condition of this contract. By executing this contract Public Agency certifies compliance with this section and each subsection and is under a continuing obligation to remain in compliance and report any non-compliance.

If this contract extends over multiple fiscal years including the initial term and all renewals, Public Agency shall confirm compliance with this section in the manner and format determined by the State by the date specified by the State and in no event later than July 1 of each year that this contract remains in effect.

If the Parties determine that any certification in this section is not applicable to this contract it may be stricken without affecting the remaining subsections.

1. As part of each certification, Public Agency acknowledges and agrees that should Public Agency provide false information, or fail to be or remain in compliance with the Standard Certification requirements, one or more of the following sanctions will apply:

- the contract may be void by operation of law,
- the State may void the contract, and
- the Public Agency or its agents may be subject to one or more of the following: suspension, debarment, denial of payment, civil fine, or criminal penalty.

Identifying a sanction or failing to identify a sanction in relation to any of the specific certifications does not waive imposition of other sanctions or preclude application of sanctions not specifically identified.

2. Public Agency certifies it and its employees will comply with applicable provisions of the U.S. Civil Rights Act, Section 504 of the Federal Rehabilitation Act, the Americans with Disabilities Act (42 U.S.C. § 12101 et seq.) and applicable rules in performance under this contract.

3 If Public Agency employs 25 or more employees and this contract is worth more than $5000, Public Agency certifies it will provide a drug free workplace pursuant to the Drug Free Workplace Act. (30 ILCS 580).

4. Public Agency certifies that the Public Agency is not participating or shall not participate in an international boycott in violation of the U.S. Export Administration Act of 1979 or the applicable regulations of the U.S. Department of Commerce. This applies to contracts that exceed $10,000 (30 ILCS 582).

5. Public Agency certifies it complies with the Illinois Department of Human Rights Act and rules applicable to public contracts, including equal employment opportunity, refraining from unlawful discrimination, and having written sexual harassment policies (775 ILCS 5/2-105).

6. Public Agency certifies it does not pay dues to or reimburse or subsidize payments by its employees for any dues or fees to any "discriminatory club" (775 ILCS 25/2).

7. Public Agency warrants and certifies that it and, to the best of its knowledge, its subcontractors have and will comply with Executive Order No. 1 (2007). The Order generally prohibits Contractors and subcontractors from hiring the then-serving Governor's family members to lobby procurement activities of the State, or any other unit of government in Illinois including local governments if that procurement may result in a contract valued at over $25,000. This prohibition also applies to hiring for that same purpose any former State employee who had procurement authority at any time during the one-year period preceding the procurement lobbying activity.

8. Public Agency certifies that information technology, including electronic information, software, systems and equipment, developed or provided under this contract will comply with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at www.dhs.state.il.us/iitaa (30 ILCS 587)