HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) DEPARTMENT OF HEALTHCARE AND FAMILY SERVICES BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is made and entered into by and between the Illinois Department of Healthcare and Family Services (HFS or Covered Entity (CE)) and _____ (Business Associate (BA)). The BA and the CE are referred to herein collectively as "Parties," or individually, as a "Party." This Agreement supplements and is made a part of the existing Contract, Community Services Agreement or other contractual agreement (hereinafter referred to as the "Contract") between the Parties.

A. Definitions

General Definitions:

Unless otherwise defined herein, the following terms used in this Agreement has the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practice, Protected Health Information, Required by Law, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

"Agreement" shall mean this Agreement.

"ARRA" shall mean the American Recovery and Reinvestment Act, Pub.L. 111–5, Feb. 17, 2009, 123 Stat. 115.

"Business Associate" generally shall have the same meaning as the term "business associate" in the Privacy Rule, 45 C.F.R. § 160.103, and, in reference to this Agreement, shall mean the entity noted above in the first paragraph.

"Covered Entity" generally shall have the same meaning as the term "covered entity" in the Privacy Rule, 45 C.F.R. § 160.103, and, in reference to this Agreement shall mean HFS.

"HHS" shall mean the Department of Health and Human Services, which is the Department of the federal government that has overall responsibility for implementing HIPAA.

"HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, Aug. 21, 1996, 110 Stat. 1936.

"HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and 164.

"HITECH" shall mean the Health Information Technology for Economic and Clinical Health Act, Pub.L. 111–5, Div. A, Title XIII, Div. B, Title IV, Feb. 17, 2009, 123 Stat. 226, 467.

"Privacy Rule" shall mean 45 C.F.R. §§ 160, 162, and Subpart E, 164.500 through 164.532.

"Security Rule" shall mean 45 C.F.R. §§ 160, 162 and Subpart C, 164.302 through 164.318.

"Secretary" shall mean the Secretary of the federal Department of Health and Human Services, or any other officer or employee of HHS to whom the Secretary delegates authority to investigate HIPAA complaints.

B. **Purpose**

ARRA, through HITECH, made significant changes to the HIPAA law and to the relationship between Covered Entities and Business Associates. BAs are now responsible for compliance with Sections 45 C.F.R. §§164.308, 164.310, 164.312, and 164.316 of the HIPAA Security Rule and the breach notification and enforcement provisions of HITECH now apply to BAs in the same way they apply to CEs.

The BA also must follow the Illinois Personal Information Protection Act of 2007, 815 ILCS 530/1 *et seq*. This statute applies to all entities, public and private, that handle, collect, disseminate, or otherwise deal with non-public information.

The BA may receive from, or create on behalf of HFS, information that constitutes PHI under HIPAA and its implementing regulations to perform the following activity for HFS: Activities under the Application Assistance Program
_____.

C. Permitted Uses and Disclosures by Business Associate

1. Business Associate may use or disclose PHI as permitted or required by this Agreement, or as required by law.

2. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with the Minimum Necessary requirements (and limitations) set forth in 45 C.F.R. §§ 164.502(b) and 164.514(d).

3. Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the CE except for the specific sues and disclosures, if any, set for in this Agreement.

4. Business Associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

5. Business Associate may provide data aggregation services relating to the health care operations of the CE.

6. Business Associate may disclose protected health information to report violations of law to appropriate federal or state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

D. **Obligations and Activities of the BA**

1. Appropriate Safeguards: The BA shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164, to prevent use or disclosure of CE's protected health information other than as provided for by this Agreement.

2. Risk Assessments: The BA shall conduct, pursuant to 45 C.F.R. § 164.308, an accurate and thorough risk assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic health information held by the BA, which shall be made available to the CE upon request.

3. Agents and Subcontractors: The BA shall ensure, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, that any agents or subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

   To the extent that the BA uses an Electronic Health Information Exchange, a Regional Health Information Organization Personal Health Record vendor, or E-Prescribing gateway, in relation to CE, the BA must enter into a contract or business associate agreement with that organization.

4. Client Access to Protected Health Information: The BA shall make protected health information in designated record sets available to CE clients within five business days of a request by a CE client or by the CE on behalf of a client. The BA also shall make PHI in designated record sets available to the CE as necessary to satisfy CEs' obligations under 45 C.F.R. § 164.524.

5. Amendment of Protected Health Information: The BA shall make any amendment to protected health information in a designated record set as directed or agreed to by the CE pursuant to 45 C.F.R. § 164.526 or take other measures as necessary to satisfy

CE's obligations under 45 C.F.R. § 164.526. The BA shall respond to a request for amendment that the BA receives directly from a client or from CE on behalf of a client within five business days. The BA shall incorporate any amendment to information in a designated record set within five business days of responding to a request for amendment. The BA shall notify the CE of a client's request for an amendment and the BA response to the request (*e.g*, grant or deny the request) within five business days of responding to the request for amendment.

6. Accounting Rights: The BA shall maintain and make available the information required to provide an accounting of disclosures to the CE's clients as necessary to satisfy CE's obligations under 45 C.F.R. § 164.528. The Business Associate shall respond to such a request within five business days of receipt of the request. At a minimum, such information shall include:

    a) the date of disclosure;
    b) the name and address (if known) of the entity or person that received the protected health information;
    c) a brief description of the protected health information disclosed; and
    d) a brief statement of the purpose for the disclosure that reasonably informs the client of the basis for the disclosure, a copy of the client's authorization, or a copy of the written request for disclosure.

7. Accounting for Electronic Medical Records: If the BA maintains an electronic medical record of a client's protected health information, the BA shall make available to the client all electronic disclosures, including those for treatment, payment, or healthcare operations, for a period not to exceed three years prior to the date on which an accounting is requested. If the BA's electronic records do not comprise three years of data, the BA shall provide the disclosures for the time period in which such electronic data exists.

8. Federal Government Access to Medical Records: The BA shall make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules. The BA shall provide CE with any information and materials provided to the Secretary at the time it is provided to the Secretary.

9. Performance of CE's Obligations: To the extent the business associate is to carry out one or more of the CE's obligations under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the CE in the performance of such obligations.

10. Retention of Protected Health Information: The BA shall retain the CE's PHI, including documentation of all unauthorized disclosures, while this Agreement is in effect, and securely maintain the PHI for a period of six years from the date of the

record's creation or the date the Agreement was last in effect, whichever is later, or as required by law. This obligation shall survive the termination of this Agreement.

11. Training: The BA shall train all its employees who access, use, modify, or disclose the CE's PHI regarding HIPAA and HITECH privacy, security, and breach notification procedures. The BA shall maintain training records, including attendance records and training materials, to be made available to the CE upon request.

12. Destruction of Protected Health Information: The BA shall implement policies and procedures for the final disposition of the CE's PHI maintained in electronic media, or any other form or medium, to make the data unusable, unreadable, or indecipherable to unauthorized individuals.

13. Breach Notification: The BA shall notify CE by email and by Registered Mail within 24 hours of becoming aware of any use or disclosure of protected health information, that is not provided for by this Agreement, including breaches of unsecured protected health information as required at 45 C.F.R. § 164.410, and any other security incident. The BA will pay all expenses related to breaches chargeable to it and hold CE harmless for any such expenses. The BA will work with the CE to ensure that all breach notifications to CE clients and others meet legal requirements.

    a) The BA's notice to CE shall identify each individual whose protected health information has been or is reasonably believed by the BA to have been, accessed, acquired, or disclosed without authorization.
    b) For purposes of this section, a data breach shall be treated as discovered by the BA as of the first day on which such breach is known or should reasonably have been known to it.
    c) For each data breach chargeable to the BA, the BA shall notify each individual whose protected health information has been accessed, acquired, or disclosed as a result of such breach.
    d) All notifications of a data breach involving PHI or PHI combined with personal identifiers shall be made in the most expedient way possible and without unreasonable delay, but in no case later than 60 calendar days after the discovery of such breach by the BA.
    e) The BA shall have the burden of demonstrating that all notifications were made as required under this section, including evidence demonstrating the necessity of any delay.
    f) Breach notification shall be provided as required by law.

14. Audits, Inspection and Enforcement: The BA shall allow the CE or its designated agent(s) to inspect the BA's facilities, systems, books, records, agreements, policies and procedures to the extent the CE determines an examination of the BA's privacy or security practices is necessary to comply with the CE's legal obligations. An inspection by the CE or its agent(s) also will be allowed by the BA to determine

whether the BA's privacy and security practices comply with the HIPAA Rules, this Agreement or any applicable law. Nothing in this paragraph shall be construed as requiring the CE to conduct any such examination.

Within five business days of a written request by CE, the BA shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of CE's PHI.

The fact that the CE inspects, fails to inspect, or has the right to inspect the BA's facilities, systems, books, records, agreements, policies and procedures does not relieve the BA of its responsibility to comply with this Agreement, HIPAA, or HITECH. The CE's detection of, or failure to detect, issues of non-compliance shall not constitute acceptance of such practice or a waiver of the CE's enforcement rights under this Agreement.

15. Safeguards during Transmission: The BA shall use security measures as required by the Security Rule to reasonably and appropriately maintain and ensure the confidentiality, integrity, and availability of the CE's PHI transmitted to the CE, the BA's subcontractors or any third party, pursuant to this Agreement and in accordance with the standards and requirements of HIPAA and HITECH.

16. Contractual Breach by the BA's Subcontractor: If the BA knows of a pattern of activity or practice of its subcontractors that constitutes a material breach or violation of the BA's agreement with the subcontractor, the subcontractor must take reasonable steps to cure the material breach. If attempts are unsuccessful, the BA must terminate the contract, business associate agreement or other arrangement with the subcontractor. If the BA believes termination is not feasible, the BA must inform CE of the problem in writing. The CE may require the BA's agreement with its subcontractor be terminated or inform the Secretary of the breach or violation.

E. **Obligations of HFS**

1. The CE shall comply with HIPAA and HITECH security standards when transmitting PHI to the BA.

2. The CE shall provide a copy of its Notice of Privacy Practices to the BA and notify the BA of any limitation(s) in the notice of privacy practices under 45 C.F.R. § 164.520, to the extent such limitation may affect the BA's use or disclosure of protected health information.

3. The CE shall notify the BA of any changes in, or revocations of, the permission by an individual to use or disclose his or her protected health information, to the extent such changes may affect the BA's use or disclosure of protected health information.

4. The CE shall notify the BA of any restriction on the use or disclosure of protected health information that the CE has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent such restriction may affect the BA's use or disclosure of protected health information.

5. The CE shall notify the Secretary as required by law of data breaches chargeable to the CE or the BA.

F. Term and Termination

1. Term: This Agreement shall be effective upon its full execution, and shall terminate upon termination with or without cause of the Contract; the execution of a new Agreement; or on the date the Agreement terminates with "notice" or "for cause" as authorized in paragraph s (2) and (3) in this Section, whichever is sooner.

2. Termination for Cause: The Business Associate authorizes termination of this Agreement by the CE, if the CE determines the BA has violated a material term of the Agreement. If the CE elects not to terminate the Agreement, the BA shall cure the breach or end the violation within 30 calendar days of the CE's election. If the BA fails to cure the breach or end the violation within the 30 calendar days, the CE may either terminate the Agreement or report BA's breach or violation to the Secretary.

   Notwithstanding termination of the Agreement, and subject to direction from the CE, the BA shall take all reasonable and necessary actions to protect and preserve protected health information and property containing protected health information in the possession of the BA.

3. Termination on Notice: This Agreement may be terminated by either Party for any or no reason upon thirty (30) days' prior written notice to the other Party.

4. Obligations of Business Associate Upon Termination: Upon termination of this Agreement for any reason, the BA shall return or, if agreed to by the CE in writing, destroy all protected health information received from the CE, or created, maintained, or received by the BA on behalf of the CE, that the BA maintains in any form. The BA shall retain no copies of the protected health information. The BA shall provide the CE with an opportunity to review the protected health information prior to its

destruction. The BA shall certify in writing to the CE that the protected health information has been destroyed.

To the extend the CE and the BA determine that returning or destroying the CE's protected health information is not feasible, there shall be written notice to the CE of the conditions making return or destruction infeasible. The BA shall continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 to prevent use or disclosure of the protected health information for as long as the BA retains the protected health information.

The BA also shall obtain or ensure the destruction of the CEs protected health information created, received, or maintained by its subcontractor(s) pursuant to the terms of this section.

G. Miscellaneous

1. No Waiver of Immunity: No term or condition of this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Federal Tort Claims Act, 28 U.S.C. § 2671 *et seq.*, or the common law, as applicable, as now in effect or hereafter amended.

2. Disclaimer: The CE makes no warranty or representation that compliance by the BA with this Agreement, HIPAA or HITECH will be adequate or satisfactory for the BA's own purposes, regarding the security or privacy of its systems.

3. Regulatory Reference: A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

4. Amendments: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of HIPAA Rules and any other applicable law. The Parties further agree to promptly enter into negotiations concerning amendment(s) to this Agreement upon request. All amendments must be in writing and signed by the Parties.

5. No Third Party Beneficiaries: Nothing express or implied in this Agreement is intended to confer any rights, remedies, obligations or liabilities whatsoever upon any person other than the CE, the BA, and their respective successors or assigns.

6. Effect on Contract: This Agreement is incorporated into the Contract as if set forth in full therein. The Parties expressly waive any claim or defense that this Agreement is not a part of the Contract between the Parties.

7. Interpretation and Order of Precedence:

    a. This Agreement supersedes and replaces any previous, separately executed Business Associate Agreement between the Parties.

    b. This Agreement is the complete agreement of the Parties with respect to their BA relationship under the HIPAA and HITECH regulations.

    c. This Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and HITECH.

    d. Any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and HITECH.

    e. In the event of any conflict between the mandatory provisions of HIPAA and HITECH and the provisions of this Agreement, HIPAA and HITECH shall control. Where the provisions of this Agreement differ from those in HIPAA and HITECH, but are nonetheless permitted by HIPAA and HITECH, the provisions of this Agreement shall control.

8. Notice: Unless otherwise specified in this agreement, all required notices between the Parties shall be in writing and shall be hand delivered or sent by U.S. Registered Mail to the representatives at the addresses below. Any notice given to a Party under this Agreement shall be deemed effective upon: (i) delivery, if hand delivered; or (ii) the fifth business day after being sent by Registered Mail.

Department of Healthcare and Family Services Representative:

Name: George Jacaway

Title: Bureau Chief

Organizational Unit: Bureau of All Kids

Email Address: George.Jacaway@illinois.gov

Address: 201 South Grand Avenue East

Springfield, IL 62763-0001

Business Associate Representative:

Name _____

Title: _____

Agency/Organization: _____

Email address: _____

Address: _____

_____

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement as of the Agreement effective date.

Department of Healthcare and Family Services	Business Associate Representative [Agency/Organization Name]
_____	_____
Elizabeth M. Whitehorn, Director	
_____	_____
Date	Date