INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE STATE OF [NAME OF STATE], [NAME OF STATE AGENCY]

AS THE STATE TRANSMISSION/TRANSFER COMPONENT
FOR THE STATE OF [NAME OF STATE]

I. Purpose and Legal Authority

A. Purpose

The purpose of this agreement is to establish the terms, conditions, and safeguards under which the **[Name of State]** [**Name of State Agency]** (**[ACRONYM]**), as a State Transmission/Transfer Component (STC) for the State of **[Name of State]** (State), will serve as a conduit between the Social Security Administration (SSA) and the specified State agencies that receive SSA data for administration of their health and income benefit programs.

Each [State agency/State] that will receive SSA data through the STC has entered into an information exchange agreement ([State Agency IEA/State IEA]) with SSA, which sets forth the terms, conditions and safeguards under which SSA agrees to disclose an identified set of data to that [State agency/State's State agencies]. The role of the STC under this agreement is limited to that of a conduit, responsible for transmitting/transferring only the authorized data files between SSA and the applicable State agencies.

B. Legal Authority

SSA's authority to enter into this agreement is section 1106 of the Social Security Act (42 U.S.C. § 1306), the Privacy Act of 1974, as amended (5 U.S.C.§ 552a(b)(3)), and SSA's disclosure regulations promulgated at 20 C.F.R. § 401.150. Disclosure of tax return information to a State agency is strictly prohibited unless the disclosure is explicitly authorized by 26 U.S.C. § 6103.

II. Responsibilities of the Parties

A. STC's Responsibilities:

1. The STC will transmit/transfer data files it receives from the State agencies to SSA and transmit/transfer data files it receives from SSA to the State agencies identified in this agreement. The data files will be transmitted directly between

SSA and the STC via SSA File Transfer Management System (FTMS) or another secure mechanism approved by SSA;

2. The STC will transfer only the authorized data files to the appropriate State agencies, as specified in Section III below. The STC will not transfer SSA data to any other agency or entity by any means without an approved modification to this agreement allowing such data transfer;

3. Upon notification from SSA that a State agency has breached or terminated its agreement with SSA, the STC will immediately discontinue transferring SSA data to that State agency; and

4. The STC will comply with the terms, conditions, and safeguards of this agreement, including its Data Protection Provisions set out below.

B. SSA's Responsibilities:

1. SSA will receive the State agencies' data files through the STC; and

2. SSA will provide SSA data files to the State agencies through the STC.

III. Transfer of Data

The STC will transfer to the State agencies listed below only the authorized SSA data system files as listed below:

State Agency	SSA Data System File
[*List each State agency to transmit data via the STC*]	**[*From Attachment A, enter the data system file(s) the agency will receive. This should match the data system files listed on the State Agency IEAs with SSA.*]**

IV. Data Protection Provisions

A. Restriction on Use, Duplication, Redisclosure, Retention, and Destruction of Data

1. The STC may not use the information contained in SSA's data files for any purpose, in any way, nor expand access to any other persons or parties without an approved modification to this agreement.

2. The STC will not use, duplicate, or redisclose the SSA data disclosed under this agreement except as provided in this agreement or as set forth in a separate State Agency IEA between SSA and the STC. STC personnel who access, use, duplicate, or redisclose the data obtained pursuant to this agreement in a manner or for a purpose not authorized by this agreement may be subject to civil and criminal sanctions under applicable Federal statutes.

3. The STC agrees to transmit the data only between SSA and the authorized State agencies listed in Section III.

4. SSA data files provided to the STC under this agreement remain the property of SSA. The STC will retain SSA data files only for the period of time required for successful transfer/transmission to the State agencies and will then destroy them.

B. Procedures for Security

1. The STC will comply with the requirements of the Federal Information Security Management Act (FISMA) (Pub. L. 107-347, Title III, section 301) as it applies to the electronic storage, transport of records between agencies, and the internal processing of records received under this agreement. SSA reserves the right to conduct onsite inspections to monitor the STC's compliance with FISMA regulations.

2. The STC will comply with the "Electronic Information Exchange Security Requirements, Guidelines, and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," in Attachment B.

3. The STC will keep complete records of each transfer of SSA data for a minimum of three (3) years and make them available for inspection as SSA may require. These records will show the date of the transfer, the recipient of the transfer, and which data files were transferred.

4. The STC will ensure that its interface software will only be used for functions specified in this agreement and will access SSA data only for the purposes described herein. SSA has the right to review the source code for the interface software to ensure that these conditions are met.

5. The STC will restrict access to the data to only those authorized State employees, contractors, and agents who need it to perform their official duties in connection with the transfer of the data files under this agreement.

6. The STC will inform personnel of the data security risks associated with their activities and their responsibilities in complying with policies and procedures designed to reduce these risks.

C. Safeguarding and Reporting Responsibilities for Personally Identifiable Information

1. The STC will inform their employees, contractors, and agents that the data may contain protected Personally Identifiable Information (PII) and Federal Tax Return Information (FTI). The STC will further ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this agreement from loss, theft or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the state employee is at his or her regular duty station;
   c. properly protect laptops and ensure that other electronic devices or media containing PII are encrypted and password protected; and
   d. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee, contractor, or agent of the STC becomes aware of suspected or actual loss of PII, he or she must immediately contact the STC's Systems Security Contact identified below or his/her delegate. The STC must then notify the SSA Regional Office and SSA Systems Security Contact identified below. If, for any reason, the STC is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the STC must report the incident by contacting SSA's National Network Service Center (NNSC) at 1-877-697-4889. The STC will use the worksheet, attached as Attachment C, to quickly gather and organize information about the incident. The STC must provide to SSA timely updates as any additional information about the loss of PII becomes available. SSA will file a formal report in accordance with SSA procedures and notify the Department of Homeland Security's United States Computer Emergency Readiness Team of the suspected or actual loss of PII.

3. If the STC experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

D. Initial Review and Certification

Prior to an initial connection to SSA, the STC must provide documentation of the design of its system for obtaining information from SSA and transferring it to State agencies. SSA will provide the template for documentation of the security design plan. The STC must also document its systems security policies, procedures, and management oversight practices for monitoring its employees' access to sensitive information in an approved SSA template. SSA reserves the right to conduct an initial onsite inspection before certifying the STC's compliance with SSA's security requirements.

E. Federal Tax Information

To the extent the STC will have access to any Federal tax information (FTI) disclosed by SSA under this agreement, the STC will not use the FTI for any purpose other than to transfer or transmit such FTI to State Agencies that use it to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement programs in accordance with 26 U.S.C. § 6103(1)(8). The STC receiving FTI will maintain all FTI in accordance with 26 U.S.C. § 6103(p)(4) and the current revision of IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, available at http://www.irs.gov. Contractors and agents acting on behalf of the STC will only have access to the FTI where specifically authorized by 26 U.S.C. § 6103 and the IRS Publication 1075.

V. Reimbursement

This agreement sets forth the terms, conditions, and safeguards under which the STC will serve as a conduit between the SSA and the State agencies that receive SSA data for administration of their health and income benefit programs under separate State Agency IEA(s). Such State Agency IEA(s) define the terms under which SSA will provide information to each state, including provisions for any reimbursement of costs.

This agreement does not cover any fees that the STC may charge the State agencies for services it provides under this agreement. The State agencies will be solely responsible for such STC fees. Any reimbursement between SSA and the State agencies will be independent from any such fees.

VI. Duration, Modification, and Termination of Agreement

A. Duration

The effective date of this agreement is July 1, 2012. This agreement will remain in effect for a period of five (5) years and will expire on June 30, 2017, unless terminated earlier.

B. Modification

The parties may modify this agreement at any time by a modification in writing signed by both parties.

C. Termination

1. The parties may terminate this agreement at any time upon mutual written consent.

2. Either party may unilaterally terminate this agreement upon 90 days advance written notice to the other party requesting termination. Such unilateral termination will be effective 90 days after the date of the notice or at a later date specified in the notice.

3. SSA may immediately and unilaterally suspend the data flow and/or terminate this agreement if SSA:

   a. determines that the STC has incurred an unauthorized use or disclosure of SSA data; or

   b. determines that the STC has violated or failed to follow any terms or conditions of this agreement; or

   c. has reason to believe that the STC has breached the data protection provisions until such time as SSA makes a definite determination of such breach.

VII. Persons to Contact

A. SSA Contacts

_____ Regional Office:

[Name], [Title]
[Office/Branch]
[Street Address]
[City, State, Zip Code]
[Phone Number]
[Fax Number]
[Email Address]

Data Exchange Issues:

Keisha Mahoney, Program Analyst
Office of the General Counsel
Office of Privacy and Disclosure
617 Altmeyer
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-9048
Fax: (410) 594-0115
Email: Keisha.Mahoney@ssa.gov

Systems Issues:

Sherri Cooper
Office of Earnings, Enumeration & Administrative Systems
DIVES/Data Exchange Branch
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0066
Fax: (410) 966-3147
Email: Sherri.Cooper@ssa.gov

Systems Security Issues:

Michael G. Johnson, Director
Office of Information Security Compliance
Division of Compliance and Oversight
3840 Annex
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0266
Fax: (410) 597-1449
Email: Michael.G.Johnson@ssa.gov

B. STC Contacts

Agreement Issues:	**Technical/System Security Issues:**
[Name], [Title]	[Name], [Title]
[Office/Branch]	[Office/Branch]
[Street Address]	[Street Address]
[City, State, Zip Code]	[City, State, Zip Code]
[Phone Number]	[Phone Number]
[Fax Number]	[Fax Number]
[Email Address]	[Email Address]

VIII. Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this agreement.

SOCIAL SECURITY ADMINISTRATION
REGION [REGION NUMBER]

_____
[Name of Signatory]
Regional Commissioner

[NAME OF STC]

_____
[Name of Signatory]
[Title of Signatory]

Attachment A – Authorized State Data Exchange Systems
Attachment B – Electronic Information Exchange Security Requirements, Guidelines, and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
Attachment C – Worksheet and Instructions for Reporting Loss or Potential Loss of PII