SSA Contract Training

Agreement Between the Social Security Administration and the NC Dept of Health and Human Services

https://medicaid.ncdhhs.gov/medicaid-training-resources-county-staff

September 2017

Justification of SSA Agreement

- Assist the State Agency to accurately determine entitlement and eligibility for state-funded benefits programs
- More economical, efficient, and faster than manual process
- Administrative savings for State and SSA

Purpose of SSA Agreement

Establish terms, conditions, and safeguards under which:

- SSA will disclose certain information to assist in administering certain federally funded state-administered benefit programs such as:
  - Medicaid
  - SSI (SDX),
  - Temporary Assistance to Needy Family (TANF)
  - Supplemental Nutrition Assistance Program (SNAP)
- State agencies to use the information **ONLY** for administering specified federally-funded benefit programs:
  - Verification of income to determine eligibility,
  - Verification of SSN/Citizenship of applicants/recipients to determine entitlement program
  - Establishing safeguards against unauthorized use and redisclosure of information by the State

Legal Authority for Disclosure

- SSA can disclose data necessary for administration of the following Federally funded programs:
  - Medicaid
  - TANF
  - SNAP (formally Food Stamps)
  - Special Assistance
  - Child Support
  - Child Care Services
  - Emergency Assistance
  - Low Income Energy Assistance Programs (LIEAP)
  - Crisis Intervention Programs (CIP)
  - Other Energy Assistance Programs

Authorized Data Exchange Systems

- **BEER** – Beneficiary Earning and Exchange Record
- **BENDEX** – Beneficiary and Earning Data Exchange
- **LIS** - Low Income Subsidy
- **Medicare 1144** – Outreach
- **PUPS** – Prisoner Update Processing System
- **QC** – Quarters of Coverage
- **SDX** – SSI State Data Exchange
- **SOLQ/SOLQI** – State On-line Query/Query-Internet
- **SVES** – State Verification and Exchange Systems, which provides SSN and citizenship verification

Legal Authority for Disclosure and Collection of Data Includes:

- Income and Eligibility Verification Data
- Tax Return Data
- Prisoner and Death Data
- Quarters of Coverage Data (for certain aliens and certain defined Federal and State benefits)
- Citizenship Data
- Administer other programs compatible with SSA programs

Agreement Regarding Verification of SSN

- The State will require each applicant or recipient to furnish his/her SSN or identifying information for administration of the programs
- SSA will in turn verify the SSN provided

System Operations and Matching

- **BEER** – Employer data for the last calendar year
- **BENDEX** – Primary source for Title II eligibility, benefits and demographic data
- **LIS** – Data from Low-Income Subsidy Applications for Medicare Part D beneficiaries
- **Medicare 1144** – List of individuals on SSA roles, who may be eligible for medical assistance for Medicare cost-sharing
- **PUPS** – Confinement data received from state and local institution (jails, prisons, penal institutions, correction center)
- **Quarters of Coverage** – SSA public information documents to determine entitlement to received SNAP
- **SDX** – file from SSA of SSI and SVB indicating termination or change in status
- **SOLQ/SOLQI** – Real-time online system that provides SSN verification
- **SVES** – A batch system that provides SSN and citizenship verification

Procedures for Notice

- Applicants
  - State Agencies will notify all individuals who apply for federally-funded, state administered benefits that any information provided is subject to verification
- Beneficiaries/Recipients
  - State Agencies and SSA will provide subsequent notices to retirees, annuitants, beneficiaries and/or recipients that information is subject to verification, including redeterminations and reenrollments

Verification and Opportunity to Contest Match Data

- State Agency will not terminate, suspend, reduce, deny or take other adverse action against an applicant or recipient based on information disclosed by SSA until the individual is notified in writing of the potential adverse action and provide the opportunity to contest the planned action
- State Agencies may use SSA's data without independent verification, with the exception of prisoner and death data

SOLQ Amendment

- This amendment establishes conditions and methods of access under which SSA agrees to extend SOLQ (online inquiry) to the State to facilitate the administration of Medicaid, Special Assistance, TANF (including Child Care), and Food and Nutrition Services programs
- Any unauthorized use or disclosure by the State and/or their contractors could result in an immediate termination of SOLQ arrangements by SSA

Agreement to Safeguard Personally Identifiable Information (PII)

- The State Agency will ensure that **Employees, Contractors, and Agents**:
  - Properly safeguard information furnished by SSA under this agreement to prevent loss, theft or inadvertent disclosure
  - Understand that they are responsible for safeguarding this information at all times, regardless of whether they are at their regular work station
  - Laptops and other electronic devices/media containing PII are encrypted and/or password protected

Agreement to Safeguard SSA Personally Identifiable Information (PII) – Cont.

- The State Agency will ensure that **Employees, Contractors, and Agents:**
  - Send emails containing PII information only if encrypted
  - Limit disclosure of the information and details relating to a PII loss only to those with need to know

Security Awareness and Employee Sanctions

Each agency must designate a department or party to take the responsibility to provide ongoing security awareness training for employees who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee's responsibility for proper use and protection of SSA-provided information including its proper disposal
- Security incident reporting procedures

Security Awareness and Employee Sanctions – Cont.

- Basic understanding of procedures to protect the network from malware attacks
- Spoofing, Phishing, and Pharming scam prevention
- The possible sanctions and penalties for misuse of SSA-provided information

SSA requires agencies to provide security awareness training to all employees and contractors who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires agencies to certify that each employee or contractor who views SSA-provided data also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure.

Limitations On Use, Duplication and Redisclosure of SSA Information

- State Agencies will use and access SSA data only for the purpose of verifying eligibility for the specific federally-funded benefit programs specified above (Slide 4)
- State Agencies will not use or redisclosed SSA data for any purpose other than to determine eligibility for benefits under the State-administered income/health maintenance programs specified above (Slide 4)
- State Agencies will not use data disclosed by SSA to extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs specified above(Slide 4)

Limitations On Use, Duplication and Redisclosure of SSA Information – Cont.

- State Agencies will use tax return information disclosed by SSA only to determine individual eligibility for specified benefit programs:
  - Contractors/agents will have access to tax return data only where specifically authorized in this agreement.
- State Agencies will only use the citizenship status data disclosed by SSA for the purpose of determining eligibility to Medicaid and NC Health for new applicants
- State Agencies will restrict access to SSA information to only those authorized State employees, contractors, and agents who need such information to perform their official duties in the intended uses as specified in the agreement

Limitations On Use, Duplication and Redisclosure of SSA Information – Cont.

- State Agencies will enter into a written agreement with each of their contractors/agents, who need SSA data to perform their duties, to abide by all laws, restrictions, use and disclosure, and security requirements:
  - Agencies will also obtain a current list of the contractors/agent employees with access to SSA data. List will include name and address of the firm, description of work and location of work site
  - Employees, contract/agent who access, use, or disclose SSA data in a manor or purpose unauthorized may be subject to civil and criminal charges
- Files shall not be duplicated or disseminated, without prior written approval from SSA, for any purpose other than to determine eligibility to federally-funded benefits. SSA will not give permission unless the redisclosure is required by law

Penalties for Disclosure of SSA Information

- It is unlawful for State Agency employees, employees of contractors/agents, and former employees to willfully disclose any information, print or published, that is unauthorized. Any violation shall be a felony punishment of:
  - In any amount not exceeding $5,000 for each occurrence of a violation
  - Imprisonment not exceeding 5 years
  - Or both, together with cost of prosecution
  - Dismissed or discharged from employment upon conviction

Information Systems Security Guidelines for Federal, State and Local Agencies

- If outside agencies (those contracted by DHHS or the county DSS to conduct specific eligibility determinations or agency employees working offsite) who have access to SSA data, all such outside agencies must provide:
  - Written description of system configuration and security features
  - Automated audit trail – The State and SSA will record every online request submitted through any and all SSA data systems
  - Access control that limit access to SSA information to only those users authorized based on their official duties
  - Monitoring user activity
  - Ongoing management oversight and quality assurance
- All outside agencies are subject to review/audit. Contractors or agency employees working offsite will be subject to both initial and recurring no-notice reviews within their work area at all times, conducted by members of the county DSS office and/or members of the NC DHHS

Reporting Loss or Potential Loss of Personally Identifiable Information (PII)

The County Security Official is responsible for reporting all incidents, regardless of severity, within one hour to the DHHS Privacy and Security Office (PSO) via their website at http://ncdhhs.gov/pso/security.htm. On the left side, click on “Report Incident”.