

# Security Awareness Training for Information Provided by the U.S. Social Security Administration (SSA)

Prepared for the  
Kansas Eligibility Enforcement System  
(KEES)

# Sensitivity of SSA-Provided Information

- Under Section 1137 of the Social Security Act (42 U.S.C. § 1320b-7), SSA provides states with information to assist with eligibility determinations
  - These disclosures must be made in accordance with the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a, CMPPA)

# Types of Data Provided by SSA

- Personally Identifiable Information (PII) such as names, Social Security Numbers (SSNs), addresses, benefit amounts, and earnings information
- Tax return data
- Prisoner data
- Death data
- Quarters of coverage data
- Citizenship data
- Other data necessary to administer programs compatible with SSA programs

# Rules on Use & Security for Processing of SSA Data

- SSA Data disclosed to the State for a specific program can be used only for that program
- State's use of SSA data must comply with:
  - the Privacy Act, as amended by CMPPA;
  - Office of Management and Budget (OMB) guidelines;
  - Federal Information Security Management Act of 2002 (FISMA);
  - National Institute of Standards and Technology (NIST) guidance;
  - Internal Revenue Service (IRS) Publication 1075; and
  - Additional requirements as agreed upon by the federal government and the State.
- Please contact Information Technology (IT) or Legal Services for more information regarding these laws and guidelines

# Rules on Use & Security – cont'd

- State will use and access SSA data only for purposes of verifying eligibility for federally funded programs administered by the State
  - Will not use or redisclose for any other purpose
  - States will not use SSA data to extract information concerning individuals who are not applicant or recipients of federally funded programs

# Rules on Use & Security – cont'd

- Rules Regarding Specific SSA-Provided Data
  - Federal tax information (FTI): Only use to determine eligibility for Medicaid/Children's Health Insurance Program (CHIP), and for Child Support Enforcement (CSE)
  - Citizenship data: Only use to determine eligibility under Medicaid and CHIP programs

# Restrictions on Viewing & Copying of SSA-Provided Information

- Access to SSA data must be restricted to authorized State employees, contractors, and agent who need the data to perform their duties
  - Contractors must contractually agree to abide by relevant laws, restrictions on access, and security requirements
  - Before contractor starts work, the State must obtain a list of current contractor employees who will have access to SSA data
    - Provide the list to SSA upon request

# Restrictions on Viewing & Copying – cont'd

- State will retain SSA data only for the required processing times for the applicable program
  - Will destroy data afterward
- State may not create separate files or records comprised solely of SSA data
- State may retain SSA data in hardcopy only as needed to meet evidentiary requirements
  - Dispose of hard copies in accordance with State's document retention guidelines



# Employee Responsibilities for Use and Protection of SSA-Provided Data

- Employees, contractors and agents of KDHE must:
  - Properly safeguard PII from loss, theft or inadvertent disclosure;
  - Understand that employees are responsible for safeguarding the information at all times, even if not at his or her regular duty station;
  - Ensure that computers or other electronic devices containing Protected Health Information (PHI) are encrypted and/or password protected;
  - Send emails containing PII only to secure addresses or, if not, then only if encrypted; and
  - Limit disclosure of the information and details regarding PII loss only to those with a need to know

# Security Incident Reporting Procedures

- If employee, contractor or agent becomes aware of suspected or actual loss of PII:
  - Immediately contact State official responsible for Systems Security
  - KEES issues should be reported to the KEES Helpdesk as a security event: 1-877-782-7358
  - State systems security official must notify SSA systems security contact within 1 hour
    - If contact cannot be reached, report the PII loss to SSA's network service center at 1-877-697-4889

# Sanctions/Penalties for Unauthorized Access, Use or Disclosure

- Employees
  - Discipline, up to and including termination
  - Civil sanctions as provided by federal law
  - Criminal charges as provided by federal law
- State
  - Loss of access to information
  - Unable to determine eligibility for federally-funded, State-administered programs