US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2016

OPDIV:

ACF

Name:

National Youth in Transition Database

PIA Unique Identifier:

P-3826761-863825

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

PIA Validation (PIA Refresh/Annual Review)

Describe the purpose of the system.

The mission of the U.S. Department of Health and Human Services (HHS) is to enhance the health and well-being of Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. As an Operating Division (OPDIV) of HHS, the mission of the Administration for Children and Families (ACF) is to promote the economic and social well-being of children, youth, families, and communities, focusing particular attention on vulnerable populations such as children in low-income families, refugees, and Native Americans. ACF directly supports HHS' Strategic Goal 3: Advance the Health, Safety and Well-Being of the American People, further supporting the three Secretary's Priorities: 1) Put Children and Youth on the Path for Successful Futures, 2) Promote Early Childhood Health and Development, and 3) Ensure Program Integrity, Accountability and Transparency. The Children's Bureau (CB), as a Program Office within ACF, partners with federal, state, tribal and local agencies to improve the overall health and well-being of our nation's children and families. With an annual budget of almost $8 billion, the Children's Bureau provides support and guidance to programs that focus on: strengthening families and preventing child abuse and neglect; protecting children when abuse or neglect has occurred; and ensuring that every child and youth has a permenent family or family connection.

The National Youth in Transition Database (NYTD) supports the statutory requirement (section 477 of the Social Security Act (the Act), the John H. Chafee Foster Care Independence Program (CFCIP)) that state agencies administering CFCIP collect and report information to the Department on independent living services provided to youth transitioning out of foster care. The statute also mandates that state agencies provide information on outcomes of youth who age out of foster care. The data submitted by the child welfare agencies are used for program management, policy development, and monitoring of child welfare programs in all 50 states, the District of Columbia, and Puerto Rico child welfare programs. The statute also requires the Department to impose a penalty of between 1 and 5 percent of the state's annual allotment under CFCIP for noncompliance with these requirements.

Describe the type of information the system will collect, maintain (store), or share.

State child welfare agencies report to NYTD information on youth transitioning out of foster care. States collect this information in individual case records maintained by the state child welfare agency. (ACF does not collect NYTD information directly from these individuals). States provide four types of information in the NYTD file: basic demographic information about youth, characteristic information about youth, independent living services provided to youth, and outcomes information provided by youth through a survey. The service information encompasses the following supports paid for or provided to youth by state child welfare agencies administering CFCIP: independent living needs assessment, academic support, post-secondary educational support, career preparation, employment programs or vocational training, budget and financial management, housing education and home management training, health education and risk prevention, family support and healthy marriage education, mentoring, supervised independent living, and financial assistance.

The basic demographic information includes an encrypted record number, date of birth, race, and sex. Characteristic information includes delinquency, tribal membership, educational level, and special education. In terms of outcomes, states must survey youth who are or were in foster care at ages 17, 19 and 21 about outcomes experiences in the following six areas: financial self-sufficiency, educational attainment, connections with adults, homelessness, high-risk behaviors, and access to health insurance. The states' NYTD file does not include a child's name, address, social security number, or any other personal information.

The information reported by the state agencies is through direct file transfer using secure transfer software. States have access to a web-based application, the NYTD Portal, that allows the state agency staff who have access permission to view the data for errors according to the compliance standards issued and monitored by the Department. Failure to meet NYTD compliance standards may result in a penalty assessed against the state agency. State agency staff that have access to the NYTD portal must use a state government email address and provide their first and last name. The user has the option to provide a phone number. User name and passwords are created and maintained by the system and must be changed on a regular basis. Individual child information is not viewable through the portal.

Federal users must use their PIV card to access the application and must be on a federal issued computer. Users have role-based access to certain features of the NYTD Portal depending on their primary role (system administrator, federal staff, or state agency staff) or secondary roles (Children's Bureau Data Team Member - granting access to data export module; and state manager - enabling a state user to submit data files on behalf of the state). Connections between state and federal computers meet FISMA standards for secure file transfer. The NYTD files are permanently stored for the purpose of data analysis.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Social Security Act (section 477 of the Act) mandates the statutory requirement for the John H. Chafee Foster Care Independence Program (CFCIP)), that state agencies administering CFCIP collect and report information to the Department on independent living services provided to youth transitioning out of foster care. Based on the Act and federal regulations at 45 CFR 1356.80 - 1356.86, state child welfare agencies must submit four types of information about youth: (1) basic demographic information on youth, (2) characteristic information about youth, (3) information on which services that states pay for or provide to each youth in 11 categories, and (4) outcomes data collected directly from youth. In order to determine if the agency has submitted the correct population for each of the above areas, including the information collected on 19- and 21-year-olds, a date of birth is required.

Other demographic information is collected in order to analyze youth based on other variables such as gender and race. The outcomes data is collected by state agencies via a 22-question survey asking youth about their experiences with financial self-sufficiency, educational attainment, homelessness, access to health care, connections to adults and high risk behaviors. In addition to being mandated by law, the agency uses the data to inform its policies and program rules used to oversee state child welfare agencies. Data also are used to conduct analysis of a youth's experience with and beyond the public foster care system. The data are maintained in the database in order to conduct analyses of individual states performance in serving youth over time as well as analyzing over time the experiences of youth in foster care and after they have left foster care. To do this, the data must be permanently stored.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth

Name

E-Mail Address

Phone Numbers

Education Records

Employment Status

Dates of birth are provided by state agencies serving youth, not users of the system.

Name, email addresses and user credentials are only collected from authorized NYTD Portal users.

A youth's educational level is reported by state agencies. Youth can voluntarily report their educational attainment to states via the NYTD survey. A youth's race, gender, sex and tribal membership are also collected by the state.
Youth can voluntarily report their employment status via the NYTD survey.

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Youth in foster care or youth formerly in foster

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The NYTD regulation implements the statute requiring states to collect and report information on youth transitioning out of public foster care. States that do not comply with this requirement are subject to penalties. The administrative data help identify the services states provide with federal funding and the outcomes linked to those services. Identifying and quantifying the services youth receive from states and the outcomes they experience helps the Department in measuring the performance of states in implementing their independent living programs. Doing so also serves the mission of the Department to enhance and protect the health and well-being of all Americans.

Describe the secondary uses for which the PII will be used.

The primary purpose of NYTD data collection is to meet statutory requirements to assess public child welfare agencies performance serving youth who are in foster care and who transitioned out of foster care. We also can analyze NYTD data in conjunction with other case-level information collected on the same youth from our two other reporting systems - the National Child Abuse and Neglect Data System and the Adoption and Foster Care Analysis and Reporting System - to understand a young person's movement into, through and beyond the public child welfare system. PII information is not needed or retrieved from these systems during data analysis.

Identify legal authorities governing information use and disclosure specific to the system and program.

Section 477(f) of the Social Security Act; 45 CFR 1356.80 - 1356.86

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

0970-0340; February 29, 2016

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The data is sourced at the state level where the individuals are notified of the data collected and why.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

ACF does not collect information directly from individuals, rather all information is received from state child welfare agencies. These agencies are not able to opt out of reporting NYTD data because it is required by law. States that fail to submit a NYTD file are assessed a penalty.

State staff may opt out of having a user account to access the NYTD Portal. If they do not provide the information they will not be granted access to the state view of the web-based application.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

State NYTD Portal users receive messages from the system administrator regarding system outages and downtime. If there are major changes to the application or compliance standards, these notices are distributed by the CB Deputy Associate Commissioner or the NYTD program lead to Child Welfare Directors and identified Program Managers at the state level. Federal users are notified by the NYTD program lead of system outages as well. Each individual state is responsible for its own notifications to clients based on their policies.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

System users contact the NYTD program lead or system help desk with concerns about their user account.

ACF does not collect information directly from individuals. State child welfare agencies submit data on youth transitioning out of foster care. For youth who have reached the age of majority and are not under the responsibility of the state agency, states must abide by their policies and statutes for obtaining information from young adults. States are able to report an option of “decline” if a youth refuses to participate in the survey. Data breaches of state child welfare information system are addressed according to state guidelines. Should the federal system be breached, ACF would notify the respective state. However, since the information in the NYTD database is associated with an encrypted number and contains only date of birth, it would nearly impossible to identify an individual youth.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

NYTD PII is not subject to periodic reviews in this system since it is information received from state child welfare agencies. ACF provides state agencies, through the web-based view, utilities that allow the agency to check their data files for accuracy. Data accuracy is a responsibility of the state agency prior to transmitting the data to ACF. ACF maintains confidentially of the NYTD files by not requiring personable identifying information beyond a date of birth. Furthermore, ACF ensures confidentiality and integrity of the files by meeting requirements for Federal Information Processing Standards (FIPS) 199 (as a “low” system) and all other cybersecurity requirements necessary to maintain its Authority to Operate (ATO). The NYTD system has completed its Security Controls Assessment (SCA) and anticipates receiving a renewed ATO this spring.

System users are responsible for maintaining accurate information on their user account.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Federal/state system users (access to name/email/date of birth) will have access to their own information and can view state data including dates of birth.

Administrators:

System administrators for maintenance and updates to the system (access to date of birth/name/email/).

Contractors:

Contractor IT system administrators for maintenance and updates to the system. System help desk contractors may have a need to view user information to provide assistance based on the specific user (name/email) role.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

There are business rules established to have the NYTD program lead identify the limited federal system users (name/email) who have access privileges to the NYTD files (including date of birth). Access rights are role based and define levels of access. Federal users require access to the PII data in order to conduct their work; determine state compliance, provide feedback on identified errors, and conduct data analysis for reports, program feedback, etc. State users submit request for access to the NYTD program lead who assigns appropriate access based on the user's role and responsibility within the state agency. The state users receive access to the PII data only for their states in order to review and validate their data compliance reports generated and penalties determined by the NYTD system and resolve any concerns when they believe their data is accurate.

All system users will be able to access their own PII.
The program and technical administrator are privileged users with access to user management function to manage the user accounts of the NYTD system. The administrators must access PII data (Email address, Telephone number) of the user needing access to the NYTD system for creating the user accounts. The technical administrator is responsible for maintenance support of the NYTD application and is responsible for correcting technical issues/concerns reported by the state users. Technical staff under contract to ACF provide technical support for maintenance/operations of the NYTD system to address technical issues/concerns reported by the states to the help desk. Contract technical staff also are responsible for answering questions of a technical nature that come in from users to the help desk. In order to provide assistance to state users, as well as do work that they are contracted to do for the overall operations and maintenance of the system, have access to emails, phone number, and names of users as well as the youth date of birth info in the NYTD file. Only those contractors who have been through a DHHS background clearance and are subject to the confidentiality clauses of the contract may have access to PII.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Users' system access is limited to the functions and information which is essential to their job functions. Role based access ensures that the levels of access are restricted to job function. Access levels are assigned on a need to know basis, only the necessary application access required to perform their duties. All requests for a user account is reviewed by the NYTD program lead and, if granted, the user is assigned the appropriate primary/secondary role. The access is based on the user's role and responsibility with the state/federal agency/organization.
Ex: The system user with a primary role of "state user" and secondary role of "Manager" can access only the youth's PII data for their state.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

NYTD collects information from public agencies that have their own policies regarding training and system access. Federal staff and contract support staff are required to take annual security training. The training includes sensitivity to PII. Contract support staff are required to sign an additional confidentiality agreement that prohibits them from discussing CB business activities with their parent organization.

In addition, all Department users (including federal employees and contractors) must review and sign an acknowledge statement of the HHS Rule of Behavior (RoB). This acknowledgment must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgment form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. Staff are required to complete an annual HHS Information Systems Security Awareness Training, HHS Privacy Training, reading the Rules of Behavior for use of HHS Information Resource and signing the accompanying acknowledgment.

Describe training system users receive (above and beyond general security and privacy awareness training).

Not Applicable.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

NYTD records retention schedule is set based on NARA Transmittal 24, General Records Schedule (GRS) 4.3, Item 020, Disposition Authority DAA-GRS-2013-0001-0004. As noted in the transmittal the disposition of files is at the discretion of the agency if longer retention is required for business use. CB retains all data files transmitted by state child welfare agencies due to need for analysis of data over time. NYTD data are maintained in the database in order to conduct analyses of individual states performance in serving youth over time as well as analyzing over time the experiences of youth in foster care and after they have left foster care. To do this, the data must be permanently stored. Also, since the NYTD data are received from public child welfare agencies who are subject to penalties, files must be maintained for any audit needs related to compliance.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative controls, including but not limited to:
System security plan (SSP)
File backup/archive conducted by hosting agency (NIHCIT)
User manuals
Contractor Agreements

Technical Controls:
User Identification and Authorization
Passwords
Firewalls at hosting site and Department firewall for federal staff computers
Monitoring and Control scans provided by hosting agency
PIV cards

Physical controls
The NYTD server is hosted in a secure data center and can be physically accessed by only the authorized infrastructure staff from ACF/HHS can access. Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, desks, storage materials,
Security Guards employing access controls to individuals requesting facility access:
Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
All physical access to data centers by employees is logged and audited routinely.
Physical containment and isolation of Systems, Data bases, and Storage assets that collection, maintain, store, and share PII
Secured and limited access facilities: data center access and information to employees and contractors who have a legitimate business need for such privileges.
When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee.
Compartmentalization and physical separation of system components (servers, cables, storage access, off-site backup facilities and storage)
Employment of Locks, Fences, Geographic Isolation of physical system assets