US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/30/2023

OPDIV:

ACF

Name:

National Child Abuse and Neglect Data System

PIA Unique Identifier:

P-3967808-369711

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Internal Flow or Collection

Describe in further detail any changes to the system that have occurred since the last PIA.

Additional Data elements to collected were added, additional data elements are not PII :
1. Field to indicate whether the infant with prenatal substance exposure has a plan of safe care
2. Field to indicate whether the infant with prenatal substance exposure has a referral to appropriate services, including services for the affected family or caregiver .
3. New maltreatment type to identify victims of sex trafficking

Describe the purpose of the system.

The purpose of National Child Abuse and Neglect Data System (NCANDS) is to collect data on reports of child abuse and neglect, including characteristics of children and their perpetrators from all 50 states including District of Columbia and the Commonwealth of Puerto Rico.

In accordance with 1988 Child Abuse and Treatment Act amendment (42 U.S.C. 5101 et seq.) NCANDS files are collected for the purpose of data analysis and publication of national and state information about child maltreatment. The NCANDS data is a critical source of information for many publications, reports, and activities of the Federal government, child welfare personnel, members of Congress, and researchers.

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

NCANDS does not collect information directly from individuals. States submit data via an Internet portal established for secure transmission of data. States only have access to their own state-specific site; access to other state sites is blocked.

The contents of the Child file contains the following information:

-Submission Year
- State
- Report and Child ID
- County of Investigation
- Report date, source, disposition, disposition date
- Notifications from law enforcement or agency
-Age at reporting
- Date of Birth
- Sex
- Child Race or Ethnicity
- County of residence
- Living Arrangements
- Military Family Member (yes/no)
- Prior Victim (yes/no)
- Maltreatment Type
- Alcohol or Drug Abuse (yes/no)
- Types of Disabilities (yes/no)
- Behavior Problems(yes/no)
- Medical Conditions (yes/no)
- Caregiver information (not PII)
- Victim of Domestic Violence(yes/no)
- Inadequate Housing(yes/no)
- Financial Problems(yes/no)
- Receiving Public Assistance (yes/no)

The following describe the services the child may have received.
- Post Investigation Services(yes/no)
- Service date
- Family Support Services (yes/no)
- Family Preservation Services (yes/no)
- Foster Care Services (yes/no)
- Juvenile Court information such as date
- Adoption Services (yes/no)
- Case management or counseling services (yes/no)
- Education and Training services (yes/no)
- Employment services (yes/no)
- Health Related services (yes/no)
- Legal Services (yes/no)
- Housing services (yes/no)

- Pregnancy and Parenting services (yes/no)
- Disability related services (yes/no)
- Transportation services (yes/no)
- Other Services (yes/no)

- Staff Data including worker ID and Supervisor ID

- Perpetrator Data (not PII) including ID, relation (parent, caregiver), age, sex, race, military member, and maltreatment type. Up to 3 perpetrators can be stored in one Child File.

Information collected in the Agency File includes aggregate information about the number of children and families who have received services, no PII held in agency files.

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

NCANDS system contains Agency Files, which contain 26 data elements, Child Files which contain 152 data elements, and user data.

1) Child File contains case-level records for each report of alleged child abuse and neglect that received a child protective services response

2) Agency File contains aggregate counts. States submit data about the number of maltreatment allegations received, allegations that received agency response, characteristics of victims and their perpetrators, and whether services were provided.

3) User data includes user's names, business phone numbers, business email addresses, office addresses, and user credentials are for purposes of multi-factor authentication and internal contact management.

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

Yes

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

Demographic data, Employee Records, Training records, Insurance Information

Gender/Sex

User Credentials

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The NCANDS files are collected for the purpose of data analyses and publication of national and state information about child maltreatment, which would make state child abuse and neglect reporting information available.

A major product of NCANDS is the annual Child Maltreatment Report, which is the primary source of information about maltreated children who were known to child protective services agencies. NCANDS data also is used to assess states' performance on national child welfare outcomes.

User credentials are collected to control system access.

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

There are no secondary uses of PII in NCANDS.

Non-PII data in NCANDS is a critical source of information for many publications, reports, and activities of the federal government, child welfare personnel, members of Congress, and researchers. NCANDS data can be analyzed in conjunction with other case-level information collected on children reported in the Adoption and Foster Care Analysis and Reporting System.

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

NCANDS files are collected for the purpose of data analyses and publication of national and state information about child maltreatment as per the 1988 Child Abuse and Treatment Act amendment (42 U.S.C. 5101 et seq.).

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

No

Not applicable

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

0970-0424, 07/31/2026

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Sharing is covered by two Memorandum of Understanding

1) Signed MOU-Data Sharing agreement between NCANDS and NDACAN
2 Signed MOU-Data Sharing agreement between NCANDS and Children's Bureau

Describe the procedures for accounting for disclosures.

Data from NCANDS is uploaded to the NDACAN site annually. Information about the upload including the date, the number of files, and the format of files are documented in a letter and shared with NDACAN for confirmation. The letters are stored with other project documents.

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

NCANDS does not collect information directly from individuals, rather all information is received from state child welfare agencies. Users are informed that PII is necessary for account creations.

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.

State staff may opt out of having a user account to access the NCANDS Portal. If they do not provide the information they will not be granted access to NCANDS.

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

ACF does not receive this information directly from individuals. If there are major changes to the data collection, these notices are distributed by the Children's Bureau (CB) Deputy Associate Commissioner to Child Welfare Directors and identified Program Managers at the state level.

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.

Users have the ability to reach out to their NCANDS Point of Contact (POC) to update any of their contact information or if they believe their PII has been inappropriately obtained, used, or disclosed. For support the user can contact the NCANDS Technical Assistance Team at 1-844-812-9633 or support@ncands.net.

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

Accuracy:
Data accuracy is a responsibility of the state agency prior to transmitting the data to ACF. ACF maintains confidentially of the NCANDS files by not requiring personally identifiable information (PII) beyond a date of birth.

Availability:
NCANDS is hosted on Microsoft Azure Cloud which has an uptime guarantee of greater than 99 percent in their service level agreement. NCANDS utilizes the automated backup services provided by Azure. Azure SQL Database automatically performs a combination of full database backups weekly, differential database backups hourly, and transaction log backups every five minutes. These backups are stored in geo-redundant storage for 35 days. The full and differential database backups are also replicated to a paired data center for protection against a data center outage. In addition, long-term backup retention is enabled for NCANDS where the backups are retained for 3 years. NCANDS has complex passwords requirements. Passwords must be at least 8 characters in length and include one uppercase, one lower case, one number and at least one special character. Each state encrypts its identifiers. The final algorithms, devoid of individual identifiers, are held only by the state. All data at rest is encrypted using Structured Query Language (SQL) Transparent Data Encryption (TDE) and data in transmission is encrypted using Transparent Layer Security (TLS) 1.2.

Integrity:
NCANDS does not collect PII directly, state governments collect the PII and store it in their systems. The states encrypt the child file prior to uploading the data to NCANDS. Once the encrypted data is uploaded to NCANDS, data quality checks are performed to ensure the accuracy and relevancy of the data. An automated validation tool is used to check field codes, intra-record field rules, inter-record rules, field value distribution, data reporting goals, and prior year comparisons If the data does not pass the checks, the states are asked to resubmit. Once the data passes the data quality checks, it is accepted into the system and the identifiers are encrypted again to protect the privacy of the subjects and prevent improper use. Administrative access is limited to privileged users to prevent the modification or destruction of the data. All activities performed by the administrators are captured in the activity logs are part of the continuous monitoring/review process.

Relevancy:
The accuracy of state staff contact information is checked and updated annually. Outdated, irrelevant, and inaccurate accounts are removed from the system. Confirmation is done with the states.

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

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

Users include administrators, developers, indirect contractors, Contracting Officer's Representative (COR), and data team. There are business rules established to address who may access the data. Federal users require access to the PII data in order to conduct their work; provide feedback on identified errors, and conduct data analysis for reports, program feedback, etc.

Contractors are required to sign data confidentiality agreements prior to accessing NCANDS test environment. Access is granted after completion of the user account request form. The NCANDS technical assistance team reviews it and sends it for COR approval. After approval is received account is created. Every member of the NCANDS team has signed the Rules of Behavior and this information is validated by the COR.

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.

Access is limited to the functions and information which is
essential to complete job functions. Computed aggregated data is provided instead of case-level data for users who do not need access PII data.

Administrator access to systems is only provided to privileged users. Data storage access is restricted to authorized users.
State users are responsible for the input of data and are restricted to only the data for their state.

The technical team, which includes CB staff and indirect contractors, have access to all records for oversight and system operations and maintenance.

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.

Federal staff and contractor support staff are required to take
annual security and privacy awareness training. Contract support staff are required to sign an additional confidentiality agreement that prohibits them from discussing CB business activities with their parent organization. Every member of the NCANDS team has signed an ROB and this information is validated by the COR.

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?

Yes

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

NCANDS records retention schedule is set based on National Archives and Records Administration (NARA)
Transmittal 24, General Records Schedule (GRS) 4.3, Item 020,
Disposition Authority DAA-GRS-2013-0001-0004.

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

Administrative controls:
NCANDS is subject to the Office of Management and Budget approval process to renew the authority to collect data using existing data elements and to add new ones. This process occurs every 3 years. During the clearance and approval process the authority of NCANDS to continue to collect data and any potential changes are reviewed by the Office of Management and Budget, the ACF Clearance Officer, the states, and the general public. 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.

Technical Controls:
NCANDS utilizes the automated backup services provided by Azure. Azure SQL Database automatically perfoArms a combination of full database backups weekly, differential database backups hourly, and transaction log backups every five minutes. These backups are stored in geo-redundant storage for 35 days. The full and differential database backups are also replicated to a paired data center for protection against a data center outage. In addition, long-term backup retention is enabled for NCANDS where the backups are retained for 3 years. NCANDS has

complex passwords requirements. Passwords must be at least 8 characters in length and include one uppercase, one lower case, one number and at least one special character. Each state encrypts its identifiers. The final algorithms, devoid of individual identifiers, are held only by the state. All data at rest is encrypted using SQL Transparent Data Encryption (TDE) and data in transmission is encrypted using Transparent Layer Security (TLS) 1.2.

Physical controls:
The NCANDS server is hosted in Azure and can only be physically accessed by authorized staff. 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 .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.

Identify the publicly-available URL:

http://ncands.net/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null