US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/05/2024

OPDIV:

ACF

Name:

Information, Family, Outcomes, Reporting, and Management System 2.0

PIA Unique Identifier:

P-2666364-994153

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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

Yes

Identify the operator.

Contractor

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

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

Modifications/enhancements have been made to the Information Family Outcomes Reporting and Management System (nFORM) 2.0 system to accommodate the new requirements for the Testing Identified Elements for Success in Fatherhood Programs (Fatherhood TIES) evaluation. As per the new requirement:

1. The nFORM 2.0 web application will implement a modified intake workflow for Fatherhood TIES designated grantees. This workflow is designed for the purpose of recording answers to screening questions, determining Fatherhood TIES eligibility, capturing consent electronically, the ability to record social security number, and conducting random assignment for Fatherhood TIES eligible applicants within nFORM 2.

2. A new user role will be created to provide access, on a least privileged basis, for the Fatherhood

TIES project authorized staff members with access to data for the universe of clients who are eligible and have consented to participate in the Fatherhood TIES evaluation. This user role will have front end access to nFORM 2.0 from which authorized users will have the ability to request/receive a full data export of all Fatherhood TIES evaluation participants, including Personally Identifiable Information (PII). On a regularly agreed interval, the nFORM 2.0 team will make available to the Fatherhood TIES team individual English-language Portable Document Format (PDF) files of each signed Fatherhood TIES consent form.

Describe the purpose of the system.

The Healthy Marriage and Responsible Fatherhood (HMRF) program is funded by the Office of Family Assistance (OFA), within the Administration for Children and Families (ACF). OFA competitively awards HMRF grants to states, local governments, and community-based organizations (both for profit and not-for-profit). These grantees are working to help participants build and sustain healthy relationships and marriages, and to strengthen positive father-child interaction.

Projects using nFORM 2.0 have a three-part strategy to:

(1) Improve the quality and cross-site consistency of data that HMRF program grantees will collect about their operations and performance;
(2) Strengthen the capacity of grantees, who may be working
with their own local evaluators, to conduct rigorous evaluations that add to the body of evidence on program effectiveness; and
(3) Examine and analyze data across grantees to draw a “big picture” of the growing HMRF experience and its effects. nFORM 2.0 facilitates high quality data collection across grantees, streamlines performance measures reporting to ACF, and provides data for the cross-site analysis. Grantees use nFORM 2.0 to track information on applicant characteristics, program operations, client enrollment and participation, and client outcomes.

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

The following types of data are recorded in nFORM 2.0:

(1) Program applicant characteristics (demographics, financial well-being, family status, health and well-being, how applicant heard about program, enrollment reasons);
(2) Program operations (strategies used to recruit participants, practices to monitor quality, staff characteristics and qualifications, implementation challenges);
3) Enrollment and participation in program services at the individual and couple levels; and
4) Client outcomes before and after services covering five outcome domains:
-Parenting, co-parenting, and fatherhood;
-Economic stability;
-Healthy marriage and relationships;
-Personal development; and
-Program perceptions.

Client data includes: intake date, program type, population, first, middle and last name, Date of Birth, whether client was screened for intimate partner violence and screening result, mailing address, home, cell, and work phone numbers, email address, Facebook, Twitter, or other social media platform contact details, information for an additional contact(s), and any case notes.

For Fatherhood TIES evaluation clients, additional data includes electronic consent for study participation, responses to screening questions, and the client’s social security number.

Names, phone numbers, and addresses for service providers such as supporting organizations are

also recorded.

System users provide first name, last name, username (email), telephone number, and authentication method (text or telephone call) for account configuration. Additionally, user type (project administrator, site administrator, case manager, general user, and reports only), grantee location, grantee partner agency (if applicable), and access permissions are assigned and maintained within the user profile.

User credentials (username and password) for ACF employees, grantees, and contractors are maintained by nFORM 2.0. The user base may also include non-grantee organizations that are participating in the evaluation in a similar capacity as the grantees.

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

ACF uses nFORM 2.0 to facilitate high quality data collection across grantees, streamline performance measures reporting, and provide data for analysis. Grantees use nFORM 2.0 to track information on applicant characteristics, program operations, client enrollment and participation, and client outcomes. Information collected and maintained on system users is maintained temporarily. To support research efforts, ad hoc queries, and rapid responses to approved requests for data exports and analyses, the nFORM 2.0 team developed a data warehouse within the nFORM 2.0 environment. The nFORM 2.0 Data Warehouse comprises data tables and analytic files more compatible with research needs. In addition to supporting rapid requests for information and cross-grantee analyses, the warehouse supports archiving of nFORM 1.0 and 2.0 data and other research initiatives of interest to ACF.

For Fatherhood TIES evaluation clients, additional data captured specifically for the Fatherhood TIES evaluation will be shared with the Fatherhood TIES team and not be stored within the warehouse.

The following types of data are recorded in nFORM 2.0:

(1) Program applicant characteristics (demographics, financial well-being, family status, health and well-being, how applicant heard about program, enrollment reasons);
(2) Program operations (strategies used to recruit participants, practices to monitor quality, staff characteristics and qualifications, implementation challenges);
3) Enrollment and participation in program services at the individual and couple levels; and
(4) Client outcomes before and after services covering five outcome domains:
-Parenting, co-parenting, and fatherhood;
-Economic stability;
-Healthy marriage and relationships;
-Personal development; and
-Program perceptions.

Client data includes: intake date, program type, population, first, middle and last name, date of birth, whether client was screened for intimate partner violence and screening result, mailing address, home, cell, and work phone numbers, email, Facebook, Twitter, or other social media platform contact details, information for an additional contact(s), and any case notes.

For Fatherhood TIES evaluation clients, additional data includes electronic consent for study participation, responses to screening questions, and the client’s social security number.

Names, phone numbers, and addresses for service providers such as supporting organizations are also recorded.

System users provide first name, last name, username (email), telephone number, and authentication method (text or telephone call) for account configuration. Additionally, user type (project administrator, site administrator, case manager, general user, and reports only), grantee location, grantee partner agency (if applicable), and access permissions are assigned and maintained within the user profile. User credentials (username and password) are maintained by nFORM 2.0, and the user base includes ACF employees, grantees, and contractors. The user base may also include non-grantee organizations that are participating in the evaluation in a similar capacity as the grantees.

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

Yes

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

Social Security Number
Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Contact details for social media platforms
Whether the client was screened for intimate partner violence and the screening result
User credentials (email address and password)

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Grantee

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of PII collected on clients is for grantees to monitor progress through the programs, including regular contact with the client for service appointments and well-being checks.

The primary purpose of the PII collected on the system users is for account set-up and maintenance.

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

None

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

Section 413 of the Social Security Act (42 U.S.C. § 613); Section 1110 of the Social Security Act (42 U.S.C. § 1310); Improving Head Start for School Readiness Act of 2007 (42 U.S.C. § 9836) [Public Law 110–134, Section 641(c)(2)]; Child Care and Development Block Grant Act of 1990 (42 U.S.C. § 9858 et seq.) and Consolidated Appropriations Act of 2008 (Public Law

110-161, Division G, Title II, Payments to States for the Child Care and Development Block Grant); Section 429A of the Social Security Act (42 U.S.C. § 628b), as added by the Personal Responsibility and Work Opportunities Reconciliation Act.

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

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-80-0361 OPRE Research and Evaluation Project Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Other

Non-Government Sources

Public

Private Sector

Other

Identify the OMB information collection approval number and expiration date

OMB Control No.: 0970-0566, Expiration Date: 03/31/2027

Father Hood TIES:

OMB Control No.: 0970-0622, Expiration Date: 12/31/2026

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.

Prior to gaining access to any grantee PII, the nFORM 2.0 team establishes data sharing agreements with each grantee that specifies roles and responsibilities regarding nFORM 2.0 access.

Describe the procedures for accounting for disclosures.

The contractor must comply with ACF's Incident Response Policy dated July 10, 2018, including any subsequent updates, as described in their contract with the Office of Planning, Research, and Evaluation (OPRE). In the event of a suspected or confirmed incident or breach, the contractor shall: protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident; notify affected individuals only as instructed by the Contracting Officer's Representatives (CORs); report all suspected and confirmed information security and privacy incidents and breaches to the CORs, ACF Incident Response Team (IRT), and other designated stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic as defined in ACF's Incident Response Policy; and provide full access and cooperate on all activities as determined by the Government and communicated by the CORs to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

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

ACF has given grantees the responsibility for notifying individual clients that their PII will be collected and for securing Institutional Review Board (IRB) approval if needed. The nFORM 2.0 team has received an exemption from the Health Media Lab Independent Review Board to use nFORM 2.0 data for project analyses. The nFORM 2.0 team has established data sharing agreements with each grantee that specifies roles and responsibilities with regard to nFORM 2.0 access. Federal and local evaluators approved by ACF, including the Fatherhood TIES evaluation, are separately responsible for securing IRB approval and establishing data sharing agreements. For individuals with a system account who must provide PII for account creation, there is not a formal notification. However, all users can see what PII is being requested of them prior to submitting the account request form.

Clients participating in the Fatherhood TIES evaluation provide their electronic consent to participate in the evaluation as well as their social security number.

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.

Client participation and provision of PII is voluntary; therefore, when clients provide PII which is recorded in nFORM 2.0, their consent to do so is implied. System administrators and grantee staff may opt-out of providing their contact information by not requesting an nFORM 2.0 user account.

Client participation in the Fatherhood TIES evaluation and provision of PII is voluntary; therefore, when clients provide their electronic consent and PII which is recorded in nFORM 2.0, their consent to do so is explicit.

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

Should any major changes be planned for how nFORM 2.0 currently uses the data, ACF program staff will work together with the ACF Office of the Chief Information Officer to review and document the data use changes within the appropriate privacy notices. OPRE would notify the nFORM 2.0 contractor who would then notify all grantee site administrators and request that the site administrators to notify their staff. For changes that would impact system functionality or availability, all users are notified by email in advance of the planned change as well as once the change has been completed. Depending on the significance of the change, the project staff will notify grantees during office hours or on-site events.

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.

Grantee staff are responsible for working directly with clients and will handle any initial concerns regarding the accuracy of client PII. Users that require their own account PII to be corrected can do so on their own.

For concerns involving the inappropriate obtainment, use, or disclosure of PII, or inaccuracies the grantee cannot resolve, the Fatherhood TIES team and the grantee site administrator have been instructed to contact the nFORM 2.0 team as soon as possible. For any suspected or confirmed incidents, the contractor will follow internal incident response procedures, which includes notification to their ACF/OPRE point of contact to appropriately report to the ACF IRT.

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

nFORM 2.0 includes several features to ensure integrity, availability, accuracy, and relevance of PII in the system.

Integrity: All modifications to records within nFORM 2.0 are logged in a history table including a date and time stamp and reference to the user account that made the update.
Additionally, the edit and delete functions are reserved for a small set of privileged users to further maintain integrity.

Availability: All nFORM 2.0 data is backed-up and replicated nightly.

Accuracy: nFORM 2.0 employs standard system features on all data entry fields to increase data accuracy, including verification checks once data is entered to confirm accurate formatting and characters as well as different field types (radio buttons, drop-downs, and calendars) to limit responses to only system acceptable data.

Relevancy: All records are considered relevant for program operations and cross-grantee evaluation throughout the duration of the contract.

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.

Access to PII within nFORM 2.0 is granted using Role-Based Access Controls (RBAC). The project administrator performs the initial grantee organization set-up and allots a specific number of user accounts that can be created. Once the grantee site administrator is set-up, the grantee takes ownership of account creation and management for their staff. The project administrator also creates accounts associated with the Fatherhood TIES researcher role. The Fatherhood TIES staff do not have the rights to create accounts.

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.

The RBAC implemented within nFORM 2.0 provides only the least amount of PII access required for individuals to perform their job duties. Within a grantee organization, there are levels of access to limit users to only enter and view PII based on their account type and data permissions. Grantee site administrators assign those account types and permissions and have access to all data. The Fatherhood TIES researcher role is only assigned by a project administrator and only has rights to generate and view a report containing data on clients participating in the Fatherhood TIES evaluation.

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.

ACF staff with access to nFORM 2.0 complete and sign the Department of Health and Human

Services (HHS) Rules of Behavior (RoB) and complete annual training on cybersecurity awareness. Contractors with access to nFORM 2.0 complete and sign the nFORM 2.0 RoB and complete annual security awareness training provided by their company in compliance with Federal Acquisition Regulation (FAR) requirements and internal security policies and procedures. Additionally, the contractors sign confidentiality pledges that stipulate sanctions for non-compliance.

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

The nFORM 2.0 contractor provides system specific training to all users (including grantees and federal staff), which includes a review of nFORM 2.0 security features and the dissemination of the nFORM 2.0 user manual. The user manual includes a review of confidentiality, how data is kept secure within nFORM 2.0, and procedures for reporting security incidents. Training for the grantees occurs in person during grantee conferences and is also offered via webinar and recorded material.

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.

The PII associated with user accounts is maintained temporarily in accordance with the National Archives and Records Administration general records schedule 3.2, item 010. The business defined cutoff is 6 years after the user account is disabled or the last password change, with longer retention authorized if required.

The information collected are covered by OPRE Record Schedules, which are records retention numbers DAA-0292-2016-0014 2.1 (final reports), DAA-0292-2016-0014 2.2 (survey/focus groups), and DAA-0292-2020-0005 (clearinghouses).

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

nFORM 2.0 leverages the following controls to protect the PII: Administrative: nFORM 2.0 uses RBAC to assign user privileges to all groups of users based on their need-to-know and required job responsibilities. System training is provided to all users to include the various nFORM 2.0 security features. The nFORM 2.0 Data Warehouse is designed to provide minimum-viable access, thereby limiting users and Amazon Web Services (AWS) services to the fewest possible permissions required for fulfilling their assigned tasks. Both users and AWS services have access controlled using Identity Access Management (IAM) roles and security groups. Additional data collected by the Fatherhood TIES evaluation (electronic consent for study participation, responses to screening questions, and the client's social security number) will not be stored within the nFORM 2.0 Data Warehouse.

Technical: Data stored by nFORM 2.0 on AWS Relational Database Service (RDS) Structured Query Language (SQL) Server databases (including the Data Warehouse PostgreSQL databases) is encrypted at rest using AWS Key Management System (KMS) Customer Managed Keys (CMKs). This RDS encryption uses the industry standard Advanced Encryption Standard (AES) -256 encryption algorithm. The nFORM 2.0 web server Elastic Compute Cloud (EC2) instance volumes are also AES-256 encrypted using AWS KMS CMKs. Data in transit is secured via encrypted transport layer security (TLS) 1.2.

Additional technical controls implemented to protect PII data for the nFORM 2.0 system in the AWS cloud include: Security Groups, Network Access Control Lists (NACLs), Route Tables, and Virtual Private Cloud (VPC) flow logs.

Physical: AWS is designed to ensure that data center locations are selected to mitigate environmental risks, anticipate and tolerate failure while maintaining service levels, and critical system components are identified to maintain the availability of AWS and recover service in the

event of an outage. Physical access to the AWS data centers is restricted to authorized employees and third parties. All requests are reviewed and approved by authorized personnel. Data center access to AWS is logged, monitored and reviewed. Access to AWS server rooms is recorded by Closed-Captioned Television (CCTV), with access points being controlled by professional security staff using surveillance, detections systems, and other electronic means. Fully redundant electrical power systems are utilized in conjunction with climate control, fire detection and suppression, and leakage detection functionality to ensure all AWS systems remain operational through any environmental issues that may arise.

Identify the publicly-available URL:

https://hmrf-nform.acf.hhs.gov/nFORM

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?

Yes

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

No