US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/29/2016

OPDIV:

ACF

Name:

Information Family Outcomes Reporting & Management

PIA Unique Identifier:

P-4603504-182510

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

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.

Alteration in Character of Data

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

This new system version now collects Social Security Numbers (SSNs) for the individuals that PII is already being collected on.

Describe the purpose of the system.

The Healthy Marriage and Responsible Fatherhood (HMRF) program is funded by the Office of Family Assistance (OFA), ACF HHS. 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. The Information, Family Outcomes, Reporting, and Management (nFORM) project, sponsored by ACF's Office of Planning, Research and Evaluation (OPRE), has a three-part strategy to improve the quality and cross-site consistency of data HMRF program grantees will collect about their operations and performance; strengthen the capacity of grantees, who may be working with their own local evaluators, to conduct rigorous that add to the body of evidence on program effectiveness; and examine and analyze data across grantees to draw a "big picture" of the growing HMRF experience and its effects.

nFORM will facilitate high quality data collection across grantees, streamline performance measures reporting to ACF, and provide data for the cross-site analysis. Grantees will use nFORM to track information on participation, record data on staff experiences, and manage workshop enrollment.

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

NFORM uses several data types including: program applicant characteristics, location, social media contacts, and program operations. Grantees will record the following types of data in nFORM: program applicant characteristics including demographics characteristics, financial well-being, family status, health and well-being, how the program applicant heard about the program, and reasons for enrolling; program operations including strategies used to market to and recruit fathers and couples into their programs, practices to monitor quality, staff qualifications, and implementation challenges; enrollment and participation in program services at the individual and couple levels; and client outcomes before and after services.

The client outcomes data cover five outcome domains: parenting, co-parenting, and fatherhood; economic stability; healthy marriage and relationships; personal development; and program perceptions.

Client data (mostly PII unless otherwise specified) will include: intake date (non-PII); program (HM or RF, non-PII); population (adult couple, adult individual, or youth individual; non-PII); first and last name; date of birth; whether the client was screened for intimate partner violence and the screening result; full mailing address (street, city, state, zip); home, cell, and work phone numbers; email address; social security number (SSN), Facebook, Twitter, and other social media contacts; information for an additional contact(s); and any case notes related to the client.
Names, phone numbers and addresses for service providers such as other supporting organizations and grantee staff will also be recorded in nFORM, including the caseworker(s) assigned to each client.

System users to include ACF and Mathematica Staff (system administrators and developers), and grantees will provide a username, password, and multifactor authentication code to access the system. The following information is needed from system users (ACF and Mathematica Staff (system administrators and developers) grantee staff) to set up an nFORM user account: first name, last name, and user name; telephone number; authentication method (text or telephone call); user type (site administrator, case manager, general user); grantee location; whether the user is from grantee’ s partner agency; and access permissions (enrollment, query tool, service provider management, session series management). The site administrator account has full access. Both the case manager and the general user accounts have limited access, with the general user account more limited than the case manager account. Grantee clients do not have direct access to nFORM and therefore do not have user accounts.

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

nFORM facilitates high quality data collection across grantees, streamlines performance measures reporting to ACF, and provides data for the cross-site analysis. Grantees use nFORM to track participation information, record data on staff experiences, and manage workshop enrollment. As part of performance measure data collection, they will use three self-administered surveys completed by clients seeking services. Grantee staff generate single-use passwords during Audio Computer Assisted Self Interview (ACASI) for the client within nFORM to log into the surveys at: enrollment; the first service; and program exit. Clients complete the surveys directly. (Clients do not have access to the nFORM system). nFORM calculates quarterly results for performance measure reporting and grantee staff can add narrative to the reports in nFORM. ACF staff generate reports from aggregated non-personally-identifiable data.

nFORM collects/maintains the following PII: SSNs to access administrative data from Federal and State Criminal Justice Agencies and Grantees; State Client name for client enrollment and case management, and performance measurement, client name is needed in order to appropriately serve clients and follow-up on additional services and outcomes; Client date of birth helps determine eligibility and appropriate services and referrals - some required performance measures are based on client age; Client address, phone numbers, email and social media contacts used for client enrollment and case management, performance measurement, client contact information is needed in order to appropriately serve clients and follow-up on additional services and outcomes; additional contact information for clients as it is anticipated that some program clients may be homeless or lack permanent housing. Information on additional contacts for the client is needed so that case managers can follow-up on additional services and outcomes; case notes on client used for client enrollment and case management, case managers may need to record notes providing details about client contacts and referrals, to ensure that subsequent client contacts and referrals are based on comprehensive information for looking up a client to enter information about him or her. PII also is needed for staff to contact clients, such as reminding them of upcoming services or checking in on the clients' well-being.

De-identified records would be extremely cumbersome and difficult for grantee staff to use for their daily operations. nFORM collects the following non-PII: Intake date necessary for grantees to ensure that clients are receiving services within an acceptable time frame of their enrollment in the program, and for measuring outcomes as required; HM or RF Program, client population, applicant characteristics necessary for ensuring that appropriate services are provided, and for measuring outcomes as required; Intimate partner screening requires that grantees document whether a screening was done. However, the screening results are not displayed to protect clients; Enrollment and participation in program services, client outcomes before and after services necessary to capture detailed information about clients' program participation so that grantee staff can ensure that clients are adequately served by the program and is necessary for required performance measures.

Mathematica and ACF collects from application users to include ACF, Mathematic staff, and grantee staff: first name, last name, and user name; telephone number; and authentication method (text or telephone call). This information used to establish the users' Microsoft Azure multifactor authentication accounts. Other data elements including the user type (site administrator, case manager, general user); grantee location; whether the user is from grantee's partner agency; and access permissions (enrollment, query tool, service provider management, session series management), will help Mathematica comply with least privilege requirements and assign only the necessary level of access that is required for a user role.

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

Client data will include: whether the client was screened for intimate partner violence and the

User credentials

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

Employees

Public Citizens

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

Grantees - non government entities.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

nFORM will help grantees collect data on clients and track the clients' progress through the program, such as receiving services and completing information on the performance measures. PII will facilitate grantee staff's use of the system, such as looking up a client to enter information about him or her. PII also is needed for staff to contact clients, such as reminding them of upcoming services or checking in on the clients' well-being. De-identified records would be extremely cumbersome and difficult for grantee staff to use for their daily operations.

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

Not applicable

Describe the function of the SSN.

SSNs are used to access administrative data from the following agencies such as: National Directory of New Hires (NDNH) data from U.S. Department of Health and Human Services Administration for Children and Families Office of Child Support Enforcement (OCSE); Criminal Justice arrests and convictions data from state agencies: New York: State Division of Criminal Justice Services, Ohio: Bureau of Criminal Identification and Investigations, West Virginia: Either from the State police or the Department of Corrections. SSNs are also needed to locate sample members who are needed to located for follow-up, NFORM will use SSN to search a database that might have more updated contact information for the sample member. The last 4 digits of the SSN will be used at the beginning of the follow-up survey to verify the identity of the sample member.

Cite the legal authority to use the SSN.

Section 413 of the Social Security Act (42 U.S.C. § 613); Section 1110 of the Social Security Act (42 U.S.C. § 1310)

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, HHS/ACF/OPRE. This Notice became

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Online

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Number 0970-0460
Expiration Date: 7/31/2018

Is the PII shared with other organizations?

Yes

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

Private Sector

Designated Mathematica (contractor) project staff will have access to the data to provide technical support to grantees using nFORM.
Grantees will be collecting the data from their clients and populating nFORM.

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

There are no agreements that facilitate sharing PII.

Describe the procedures for accounting for disclosures.

The ACF NFORM Incident Response Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

ACF implements an incident response capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The Incident Response Policy and procedures are designed to coordinate incident handling activities with contingency planning and incorporates lessons learned from ongoing incident handling testing and training into incident response procedures and implements the resulting changes accordingly. The ACF NFORM Incident Response Plan has been developed and tested by the contractor security operations and technical teams and is under the supervision of the government Information System Security Officer. This plan will be tested, reviewed and updated on an annual basis in compliance with HHS IT Security mandates.

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

It is not in Mathematica’s purview to include notification of clients’ rights to participate voluntarily in the grantee program. That is the responsibility of the grantee sites who will administer the services to their clients.

Grantee staff and system administrators are made aware that their contact information is needed when they voluntarily populate the nFORM user account request form. This information is collected to establish the user’s multifactor authentication account.

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 completely voluntary; therefore, when clients provide PII which is recorded in nFORM, 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 user account.

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

The HMRF grantees funded by DHHS, Administration for Children and Families, will be responsible for recruiting, screening, enrolling, providing services, and capturing program and performance data on program clients in nFORM. Mathematica Policy Research will obtain this program and performance administrative data from grantees to support program monitoring and identify trends in client and grantee experiences during the grants. Mathematica will not have direct contact with grantee clients and has received a waiver of informed consent from the New England Institutional Review Board (IRB) for purposes of obtaining this data from grantees. After receiving the appropriate guidance from Mathematica's legal department, Mathematica will notify site administrators who will subsequently notify their grantee staff of any major system changes involving how their contact information is disclosed or used within nFORM. System administrators would determine what major system changes are required and therefore would not require additional notification.

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 will be responsible for working directly with clients and for recording PII in nFORM. Each grantee will directly handle client questions or concerns about the accuracy or security of their PII in nFORM. Grantee site administrators will contact the Mathematica nFORM project administrator with any questions about PII accuracy or security that cannot be addressed with the client. In the event that an individual is concerned that their PII has been inappropriately obtained, used, or disclosed, the nFORM project administrator will work with Mathematica's incident response team who will follow the nFORM incident response procedures to investigate the issue.

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 will include several features to ensure the integrity, availability, accuracy, and relevance of PII in the system.

Key fields are required and must be completed to proceed with a task in nFORM.
Sing skip logic, specific responses in key fields will determine whether grantee staff or clients completing surveys are asked subsequent questions.Where applicable, fields have edit checks to ensure that data are provided in the correct format. Radio buttons, drop down menus, calendar functions and other common system features are used to ensure that responses are limited to the range of acceptable data for a given item. nFORM will include a query tool which grantees can use to export selected sets of data for analysis and additional data quality checks.

Only authorized users will have the ability to edit or delete certain data elements after they are recorded in nFORM.

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

Users:

nFORM system is designed for use by multiple users including ACF staff, Mathematica contractors, and grantees, each of whom will have varying degrees of access to the system and associated data based on their user role. Grantee site administrators will be responsible for setting up and maintaining nFORM user accounts which will define each user's access to the system.

Users' login information, based on their user account, will define their level of access when using the nFORM system. Multifactor authentication will be used by the grantee staff to provide a second form of authentication for access to PII contained within certain components of the nFORM system.

Administrators:

Grantee site administrators will be responsible for setting up and maintaining nFORM user accounts which will define each user's access to the system" into the explanation response field

Contractors:

Designated Mathematica (not considered direct contractors) project staff will have access to the data on a need-to-know and least privilege basis to provide technical support to grantees using nFORM.

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

NFORM is operated by a contractor. Mathematica Policy Research enforces the most restrictive set of rights/privileges or accesses needed to use (or processes acting on behalf of users) for the performance of specified tasks. The organization employs the concept of least privilege for specified duties and information systems in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, or individuals.

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.

Mathematica nFORM developers have implemented access controls that allow for varying degrees of access to the system and associated data based on a user's role. Mathematica and grantee site administrators define these roles and the associated access when establishing user accounts to allow system login. Multifactor authentication will be used by the grantee staff to provide a second form of authentication for access to PII contained within certain components of the nFORM system for authorized users.

The organization employs the concept of least privilege for specified duties and information systems in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, or individuals.

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.

Mathematica staff received annual security awareness training that addresses the security policies and procedures contained in the Mathematica Security Manual. All contractors, must review and sign an acknowledge statement of the HHS Rule of Behavior (RoB). Staff sign confidentiality pledges that stipulate sanctions for non-compliance and complete Mathematica's online security awareness training shortly after their start date. Refresher training is delivered annually thereafter and remind staff of the relevant sanctions.

Mathematica also maintains an intranet web page with extensive information regarding security. The web page contains links to the Mathematica Security Manual and other security resources, instructions for using encryption and overwriting software, and guidance on incident reporting. As warranted, Mathematica's Information and Technology Services (ITS) department broadcasts messages to all network users regarding computer security updates. Grantee staff will complete nFORM specific training that will include nFORM security features and protocols. The training is expected to occur in person and by webinar.

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

Mathematica will provide training to grantees about nFORM in-person during a grantee conference and via webinars. The trainings will included nFORM security features, such as user restrictions. nFORM security features will also be described in an nFORM User Manual provided to grantees.

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.

General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0004. Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

PII will be retained in a manner consistent with the implemented security controls for retaining audit logs. The record retention period is for 180 days which meets the HHS audit retention standard.

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

Mathematica protects the confidentiality and integrity of information at rest. The nFORM system resides on secure servers protected with AES 256-bit encryption. Access to the nFORM is restricted through the use of ACLs. Access is granted on a need-to-know and least privilege basis. All staff who have access to PII in nFORM are trained to maintain all PII.

Mathematica's Information Services (IS) Department developed nFORM using ASP.NET Model-View-Controller 5 (MVC5), JQuery 1.10.2, and HTML5 with a SQL Server Database back-end. The web servers, running Microsoft Internet Information Services (IIS) 7.5, are encrypted with advanced encryption standard (AES) 256-bit encryption via Microsoft Encrypting File System (EFS). The database, running on a SQL Server 2008 R2, is encrypted with AES 256-bit encryption via Microsoft EFS and is audited with the Idera Compliance Manager ver. 4.3.406. Data transmitted to and from nFORM is secured via transport layer security (TLS) with AES 256-bit encryption. Mathematica's servers are equipped with uninterrupted power supplies and are stored in locked climate controlled rooms within Mathematica's locked office suite. Additional software protecting the nFORM system components include Symantec Endpoint Protection Version 12, Tenable Security Center Continuous View 5.2 (Nessus Vulnerability Scanner with Nessus Agent 6.5.4, Passive Vulnerability Scanner 4.4, and Log Correlation Engine 4.4.1), Cisco Identity Services Engine 1.2, Cisco ASA 5520 8.4.7 and Cisco ASA 5545 9.2.4 (Piscataway Datacenter).

We achieve redundancy by utilizing dedicated private circuits in our larger locations and backup virtual private network (VPN) connections at our smaller locations. All office locations are protected by a secure, proactively monitored high availability firewall. The corporate data networks and associated traffic are proactively monitored using a leading network and security management platform.

Identify the publicly-available URL:

https://www.FAMLECROSS-site.com/nFORM

https://www.FAMLECROSS-site.com/Survey

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

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.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under 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?

Yes