US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/27/2017

OPDIV:

ACF

Name:

Electronic Case Management Record System

PIA Unique Identifier:

P-9816463-555994

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Design

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

Describe the purpose of the system.

The Office of Human Services Emergency Preparedness (OHSEPR)and Response in the Administration for Children and Families (ACF) uses the Electronic Case Management Record System (ECMRS) to assist in the delivery of Federal disaster case management services through the Immediate Disaster Case Management (IDCM) services. The system allows for the following:

Rapid deployment of personnel with ready access to ECMRS that allows disaster case managers to efficiently connect victims of disasters to services and resources of multiple agencies

Integration with existing state, local, and voluntary agency programs in order to create one seamless disaster case management program

Augmentation of existing state, local, and voluntary agency programs to fill gaps by allowing for the centralization of information Scalability to any size disaster, particularly if the affected area encompasses multiple states

Configuration to align with the needs of the State/Tribe/Territory that are disaster and mission specific

The ECMRS greatly reduces respondent burden through built-in algorithms that streamlines response options and patterns. All information gathered is exclusively used to inform the delivery of disaster case management services and programmatic strategies and improvements

This system of records is being developed by an ACF direct contractor. Data is stored and managed by ACF.

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

Case Manager accounts will be established by the direct IDCM contractor through the appointed super user account. Case manager accounts will generate username and passwords through the collection of:
First Name
Last Name
Email Address
Group (specified according to the disaster activation)

Client records in the system will be initiated by a case manager. The case manager's name will become a part of the client record to track case manager to client ratios. The client record contains information to include, but are not limited to applicants' names, addresses, telephone numbers, email addresses, household size and composition, information about damaged real and personal property, degree of damage incurred, income information, information about qualification for disaster assistance, information about assistance sought and received from federal, state, local and other disaster assistance agencies, including eligibility and qualifications for disaster and other forms of assistance, health care treatment, and health insurance information (i.e., do you have insurance coverage and has the coverage been interrupted/lost as a result of the disaster?)

The different categories of information being collected through the intake assessment form are designed to best meet the needs of populations in the immediate post disaster period. The form gathers housing, transportation, employment, military status, financial, legal, language, child and youth, food, clothing, furniture and appliances, senior, and health-care related needs information as part of a comprehensive assessment. The questions are specifically designed to collect pre and post disaster information that enables the coordination of assistance for individuals and families to receive disaster relief assistance from multiple organizations providing services during a disaster event.

There will be two privileged users for the ECMRS system. The privileged users are federal employees, and they will be responsible for adding contractor's information into the system upon a request for case managers to deploy to perform IDCM services. These direct contractors will be given access to accounts via dual factor authentication.

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

OHSEPR and its direct contractor Apprio have worked together to customize a web-based system that allows for centralization of information collected with clear process-oriented work-flows. The customized dashboard enhances a disaster case manager's ability to minimize the time processing each individual impacted by a disaster. The ECMRS uses Apprio's National Disaster Medical System (NDMS) platform to collect client information. This platform solution helps improve efficiency of tasks, such as determining eligibility, developing case notes, tracking client progress, measuring outcomes, and providing referrals.

In addition to improving the information collection process, the ECMRS promotes centralization of information and resources, allowing disaster case managers to quickly connect individuals impacted by disaster with resources and services of multiple agencies. ECMRS allows configuration to align with needs of the State/Tribe/Territory that are disaster and mission specific.

The ECMRS greatly reduces respondent burden through built-in algorithms that streamlines response options and patterns. All information gathered is exclusively used to inform the delivery of disaster case management services and programmatic strategies and improvements.

The collection of information is contingent upon activation of ACF's IDCM services by the Federal Emergency Management Agency (FEMA) through its Interagency Agreement (IAA), following a Presidential declaration of a disaster. ACF's OHSEPR is following all regulatory requirements to collect and store confidential data electronically to include the Federal Risk and Authorization Management Program (FedRAMP) certification with Authorization to Operate approval. ACF will store the data with ongoing intrusion detection monitoring processes.

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

Mailing Address

Phone Numbers

Medical Notes

Military Status

Employment Status

Income

User Credentials

Personal Property Information

Household size and composition information

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

Employees

Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Collection of certain PII is needed to verify eligibility, link individuals with appropriate resources, and provide advocacy services as needed.

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

The use of an ECMRS system improves and synchronizes inter-agency communication and coordination during disaster recovery events through enhanced reporting capabilities that are available within select systems. As such, the information that is collected in the system will be examined post disaster to identify client trends, as well as areas for program and process improvement.

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

Section 426 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), as amended, 42 U.S.C. §5189d authorizes the Federal Emergency Management Agency (FEMA) and the U.S. Department of Health Services' Administration for Children and Families (ACF) to provide IDCM services under the federal Disaster Case Management Program (DCMP).

The use of the Electronic Case Management Record System (ECMRS) is aligned with Executive Order of the President 13589 and the memorandum to the Heads of Executive Departments and Agencies M-12-12 from the Office of Management and Budget to "Promote Efficient Spending to Support Agency Operations."

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.

2/09-80-0311 OHSEPR Disaster Case Management Project Records, HHS/ACF/OHSEPR

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

The Federal Register for the Immediate Disaster Case Management Intake Assessment has been posted under OMB No. : 0970-NEW.

Is the PII shared with other organizations?

Yes

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

Within HHS

Aggregate information will be shared within ACF to update ACF and HHS Leadership of disaster impacts and the status of IDCM missions.

Other Federal Agencies

The IDCM Program is based on the principle of support to states. The ECMRS will be utilized to provide immediate services, with the intent of transferring client's information to State DCM programs as soon as possible. All cases will be transferred at the end of the program.

State or Local Agencies

State Emergency Agencies

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

FEMA activates ACF via an existing Interagency Agreement (IAA). The IAA helps strengthen areas of mutual support and coordination in the development, administration, and implementation of the DCMP to maximize optimal and rapid recovery.

FEMA
Ensures disaster specific funding is made available from the Disaster Relief Funds to support the execution of the ACF IDCM program. A fully-funded Task Order to ACF under the FEMA-ACF IAA is required, covering the full planned period of activation.

ACF
The ACF Watch Desk produces weekly reports for FEMA, the State, Tribe, or Territorial and the Health and Social Services Recovery Support Function (H&SS RSF) (if activated); develops plan and coordinates the transition of all cases handled by ACF IDCM to State/Tribe/Territory.

Describe the procedures for accounting for disclosures.

When the IDCM Program is activated by FEMA, a Routine Use letter is submitted to the FEMA Federal Coordinating Officer to request access to FEMAs' database of clients that have applied for disaster assistance. Once approved, information is provided to HHS/ACF pursuant to 44 CFR 206.110(j)(1)(ii) and the “routine use” provision of the Privacy Act of 1974, 5 U.S.C. 522a(b)(3). HHS/ACF is authorized disclosure of this information under routine use (H)(1) of DHS/FEMA-008, Disaster Recovery Assistance Files, System of Records Notice, 74 Fed. Reg. 48763, 48765-6, (September 24, 2009), and HHS/ACF will not further disclose this information to any entities other than to its direct contractor. The disaster clientts' information will be protected in accordance with the Privacy Act of 1974 but will not be maintained in an HHS/ACF system of records.

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

IDCM services, to include information collection, is pursuant to a signed consent that describes how case managers use and share information provided by clients. This HHS-approved consent is in addition to any consent required by FEMA for release of information. The consent form is signed at enrollment.

Information collection is contingent on activation following a Presidential declaration of a disaster. A Presidentially declared disaster and the activation of IDCM program cannot be predicted given the unpredictable nature of disasters.

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.

Enrollment in the program is voluntary. PII must be collected to verify eligibility and for provision of services.

System administrators/users are direct contractors. The direct contractors do not have an option to object information collection. User accounts and access to the system controls will not be designated to a direct contractor who opts not to enter their information.

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

The time-frame for the duration of IDCM services is established at up180 days. Given that IDCM services are time focused, clients are not notified of any changes following the performance period period (i.e., up to 180 days).

System administrators are direct contractors and will provide their consent to create their user credentials in order to access the system and satisfy the contract requirements. All system users will complete security and privacy awareness training and must provide their consent to be given access to data generated and stored on the secured cloud storage.

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.

Contesting record procedures:

Individuals seeking to amend a record about themselves in this system of records should address the request for amendment to the System Manager. The system manager is a direct contractor working in the capacity of a case manager supervisor. The case manager supervisor can be contacted by initiating a request through the case manager assigned to the client's case. The request should include the name, telephone number and/or email address, and address of the individual, and should be signed; identify the system of records that the individual believes includes his or her records or otherwise provide enough information to enable the identification of the individual's record; identify the information that the individual believes is not accurate, relevant, timely, or complete; indicate what corrective action is sought; and include supporting justification or documentation for the requested amendment. Verification of identity as described in HHS's Privacy Act regulations may be required. 45 CFR § 5b.5 ACF and its contractors make best efforts to resolve any issues that arise with respect to notification, access, or contesting records of other organizations.

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

The Standard Operating Procedure (SOP) for ECMRS ensures the PII within ECMRS is periodically reviewed by the ECMRS program manager and system administrator. These reviews include a weekly audit to report on user account events/activities (account deletion, account changes, etc.), to ensure the integrity, accuracy and relevancy of data contained in ECMRS. Information Integrity and availability are also protected by security controls, selected from the National Institute of Standards and Technology's Special Publication 800-53. The only PII stored in the system (i.e. name,phone number and e-mail address) are provided during the registration process and are submitted by applicants. Users are responsible for ensuring that their registration information is accurate.

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

Users:

Users (i.e., disaster case managers) complete the assessment process and assist the client(s) with linkage to resources and services.

Administrators:

To generate reports, based on aggregate data.

Developers:

Direct contractors; responsible for the operations and maintenance of the system

Contractors:

Direct; system is maintained by the contractors

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

Users and administrators, as described above, have access to PII. Access is granted by select system administrators (federal staff) and only those who are directly involved in the provision and management of IDCM services.

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.

ACF users only see data at the aggregate level to avoid unintentional access to PII.

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.

Administrators of the database follow the rules of the HHS Rules of Behavior. Annual security awareness training is required, this also includes HHS Privacy Awareness Training and all ACF IDCM staff receive training on confidentiality policies and procedures, including legal requirements of the Privacy Act, and methods of protecting client confidentiality.

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

Users are trained to use the ECMRS to conduct an assessment of the individual/families impacted by the disaster.

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.

Retention of PII follows the General Records Schedule (GRS) for electronic input/source records, disposition authority - DAA-GRS-2013-0001-0004.

Final Disposition: Temporary. Destroy after six years after period of performance.

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

The HHS system security authorization process is used along with completion of the System Security Plan, Risk Assessment, Contingency Plan, Configuration Management Plan and all controls required for a Moderate Risk System. As a system hosted in the ACF Amazon Web Services (AWS) General Support System (GSS), this system inherits all the controls of the GSS as the system host. The Amazon Web Services GSS is covered by a separate, approved Privacy Impact Assessment (PIA).

Access to the systems is given based on need to know and job responsibilities. Packages such as Resource Access Control Facility (RACF) grant or deny access to data based upon 'need to know' roles. External audits also verify these controls. Technical controls used include user identification, passwords, RSA (Rivest-Shamir-Adleman) tokens, firewalls, virtual private networks and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks and closed circuit televisions.