

US Department of Health and Human Services

Privacy Impact Assessment

Date:

02/10/2017

OPDIV:

ACF

Name:

2015 LIHEAP RECS Data Match System

PIA Unique Identifier:

P-7415956-907944

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Planning

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?

No

Identify the operator.

Contractor

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.

Describe the purpose of the system.

The Low Income Home Energy Assistance Program (LIHEAP) is a federal program that provides funds to states, territories, tribes, and the District of Columbia for the purpose of providing energy assistance and weatherization to low-income households. LIHEAP is managed by the Office of Community Services (OCS) in HHS' Administration for Children and Families (ACF).

This system is the 2015 LIHEAP Residential Energy Consumption Survey (RECS) Data Match System. (2015 LRDMS). It collects existing same-year data from LIHEAP grantees (and, in some cases, sub-grantees (grantee data)) in order to match/append state data with data uploaded by the Department of Energy. The purpose is to: Identify the respondents to the 2015 REC Survey that received LIHEAP benefits, which is state communicated information; and match/append the state LIHEAP dataset to the dataset received from the Department of Energy.

This will be done by joining common data elements that exist in each dataset.

Such grantee data is that which LIHEAP grantees collect from LIHEAP applications; and aggregate for the LIHEAP Household Report. The merged data greatly enhances the accuracy of LIHEAP receipt data, which would otherwise be household-reported and therefore highly suspect. No new PII is collected. Furthermore, all PII used by the system is already authorized to be collected by the Department of Energy's Energy Information Administration (EIA).

The merged data allows OCS to gain information about program participation, program benefits, poverty status, vulnerable household status, and ethnicity on the part of LIHEAP recipients. It also allows OCS to study the impact of LIHEAP on income eligible and recipient households in accordance with the LIHEAP statute. Ultimately, it enters into the Department's annual LIHEAP Report to Congress and the annual LIHEAP Home Energy Notebook.

42 USC 8629(a) authorizes OCS to collect this information.

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

The system acquires top-coded information from the 2015 RECS sample that covers housing unit characteristics (including address and state), household characteristics (including householder name and household phone number), fuel usage characteristics, space heating and air conditioning, fuel bills, residential transportation, and home energy assistance. It gathers raw information from state administrative records--through state-specific databases--that covers household address (including state), householder name, household phone number, household size; gross income, amounts and dates of assistance receipt (including those for heating assistance, cooling assistance, crisis assistance, and other assistance), presence of vulnerable groups (including elderly persons, disabled persons, and young children), and tenure type (including heating cost inclusion in rent). It gets acquires and gathers all such information through a website that uses Secure File Transfer Protocol (SFTP).

The system, outside the agency and contractor, shares none of the information that it collects other than that which enters into the products and analyses that show program participation, program benefits, poverty status, vulnerable household status, and ethnicity on the part of LIHEAP recipients.

The contractor is, with respect to this system, a direct contractor. It is a direct contractor because all of its staff people who have or will get access to the system will access the system through HHS-issued government employee identification badges; and will have undergone the background check "National Agency Check and Inquiries (NACI)" that the receipt of such badges requires.

The system's users gain access to the system through government-owned access control software. Such software isn't part of the system. Instead it's part of the standard local area network software that gets installed on all government-owned laptops. A government-owned laptop is the only way in which the system's users gain access to such system.

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

The goal of the 2015 LRDMS is to merge 2015 RECS data with state grantee data to produce a report about LiHEAP recipient households. The data will be securely uploaded to an ACF hosted SFTP server, then transferred to an ACF hosted Stata Data server which can be accessed by OCS direct contractors to pull the data onto a government-funded Information Technology Infrastructure and Operations (ITIO) laptop via a Virtual Private Network (VPN). The data will then be merged and the final report uploaded back onto the Stata Data server.

The system collects data on household income, energy usage, dwelling characteristics, and benefit receipt. The files that are uploaded by the states that received benefits and the files uploaded by the Department of Energy, both of which contain the PII, will be deleted once the data match/appendix file is created. So the system contains PII for a temporary amount of time from the original input data. Once the data is merged, all information becomes desensitized and unidentifiable. The input data is never shared with anyone outside of the OCS direct contractors that will be performing the work. The merged data that makes up the final report contains information to show program participation, program benefits, poverty status, vulnerable household status, and ethnicity on the part of LIHEAP recipients.

The system will collect and maintain the data only temporarily. Once the final report is produced, the data will be purged from all ACF servers.

The system doesn't collect, maintain, or store any data about the system's users or user credentials.

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

Yes

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

Name

Mailing Address

Phone Numbers

Household Income

Ethnicity

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

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of the PII is to use the data elements in the grantee data to identify which households that participated in the 2015 RECS received LIHEAP assistance, so as to permit a merge of such datasets.

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

There is no secondary use for PII within the 2015 LDRMS.

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

The legal authorities for the 2015 RECS are as follows:

15 USC 764(b)

PL 93 - 275 13(b)

15 USC 764(a)

15 USC 790a

The legal authority for the grantee-sourced data is as follows:

42 USC 8629(a)

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

No

Identify the sources of PII in the system.

Government Sources

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

The OMB Control Number is 0970-0486. The expiration date is 9/30/2019.

Is the PII shared with other organizations?

Yes

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

Private Sector

APPRISE, Inc. (APPRISE) is the organization with whom PII will be shared. APPRISE is ACF's direct contractor that will build the database that comprises the system; develop the protocol for matching the records of each dataset; and carry out the manual portion of the data match.

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

The agreement that authorizes the information sharing between APPRISE and ACF is the LIHEAP Technical Support Project for FFY 2014 – 2015 (HHSP233201450049A) between APPRISE and ACF. Such agreement calls for APPRISE, Inc. to build the system and carry out the record-matching process.

Additionally, OCS has an agreement with EIA to obtain PII-containing 2015 RECS data provided it uses such data only for statistical purposes. Such agreement is covered by the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA).

Describe the procedures for accounting for disclosures.

For the state administrative data that contains the PII, OCS intends only to collect; transfer between or within agencies; use for the match; and destroy. OCS doesn't intend to disclose such data.

For the 2015 RECS data, OCS intends only to transfer from EIA to APPRISE. APPRISE has data security procedures in place to prevent unauthorized disclosure of the grantee data.

If there occurs, for reasons other than satisfaction of a Freedom of Information Act (FOIA) request, an authorized disclosure of PII outside of the system then HHS will document such disclosure within a system log that provides the following information: The date, nature, and purpose of each such disclosure; and the name and address of the recipient.

HHS shall keep such log for five years after the longer of the date on which the disclosure occurs; or the life of the record. Furthermore, if the individual named in the record requests an accounting of disclosures then OCS shall provide the details of all disclosures except for certain ones which relate to civil or criminal law enforcement.

If there occurs an unauthorized disclosure of PII outside of the system (e.g. by sending names through email) then such disclosure is recorded and a report is generated. This report describes the date, nature, and purpose of each disclosure; and the name and address of the recipient. All such reports are maintained for a period of [X] year[s] subsequent to such disclosure.

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

No such prior notice is given by HHS. That's because such individuals would have already received such notice from, as applicable, their respective grantees or EIA; the resultant data will be used only for statistical purposes (i.e., not to make decisions about any individual); and the resultant data won't contain PII.

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.

LIHEAP grantees and sub-grantees require LIHEAP recipients, as a condition for participating in the program, to consent to allowing their data to be shared for statistical purposes. Individual opt-outs from PII collection or use, and the consequences of opting out, are up to each grantee.

Such notification is excepted under 5 USC Sec. 552(b)(5).

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

For the RECS, participation by heads of household is voluntary.

For the grantee data, the system doesn't retain any data that may be specifically attributable to a individual. It uses PII only to merge state data with the RECS. After such merge, the PII is destroyed. No other uses or changes can take place.

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.

For the RECS, participation by heads of household is voluntary.

For the grantee data, the system doesn't retain any data that may be specifically attributable to an individual. It uses PII only to merge state data with the RECS. After such merge, the PII is destroyed. No other uses or changes can take place.

There is no formal process in place to address such concerns. That's because the 2015 LRDMS doesn't actually collect the PII from the individuals from whom the PII is obtained. Instead it obtains the PII from other systems, specifically those that carried out such collections. Therefore, such individuals should contact the administrators of those systems if they believed that their PII was inaccurate or inappropriately handled.

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 system holds PII, from all sources, for too short a period to warrant periodic reviews. Such period extends for not longer than one year. The PII data is part of the initial data sets uploaded by EIA and the state grantees. When the data merge occurs to produce the final report, that resultant data set no longer contains PII. After the final report is produced the all data will be purged from the ACF secure servers. No other uses or changes will take place.

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

Developers:

The direct contractor, APPRISE, makes up the developer pool of users who will have access to the PII in the system's precursor. They require such access in order to merge the records of the original datasets. They must sign a Confidentiality Agreement; agree to an Internet and Network Security Policy; and complete CIPSEA training, if they work with the 2015 RECS data. Furthermore, APPRISE only allows staff assigned to the project to have access to the data location.

Contractors:

APPRISE staff constitute the direct contractors who will have access to the PII in such system.

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

The direct contractor APPRISE only allows staff assigned to the project to have access to the data location. Such staff must sign a Confidentiality Agreement; agree to an Internet and Network Security Policy; and complete CIPSEA training, if they work with the RECS data, and clear an ACF required background check to obtain a Personal Identity Verification (PIV) badge.

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 direct contractor APPRISE only allows staff assigned to the project to have access to the data location. Such staff must sign a Confidentiality Agreement; agree to an Internet and Network Security Policy; and complete CIPSEA training, if they work with the RECS data.

APPRISE provides data submitters (State/Local/Tribal entities) a set template to prevent the accidental submission or viewing of non-project related PII (meaning other than Name, Phone Numbers, Mailing Address, Household Income, and Ethnicity) by APPRISE staff. The PII that is viewed by APPRISE staff is the minimum amount necessary to complete such staff members' assigned tasks.

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.

The direct contractor APPRISE only allows staff assigned to the project to have access to the data location. Such staff, if they work with the RECS data, must complete annual CIPSEA training; have an HHS background check at or above the level needed for the federal government building pass and computer access card; read the standards and complete the training that apply to their access; and review and sign an acknowledgment of having read and understood the HHS Rules of Behavior (RoB) for the Use of Information Resources. Such staff are the only ones who will have access to view the PII.

CIPSEA training constitutes online training modules, provided by EIA, on the appropriate handling and use of the PII (such modules appear at <http://www.eia.gov/cipsea/cipsea.html>); and (information, provided by ACF, about the existence of the CIPSEA agreement and the penalties for violation. The other training that applies to such access consists of information systems security awareness training; and privacy training. All training must be completed annually.

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

The direct contractor APPRISE only allows staff assigned to the project to have access to the data location. Such staff, if they work with the RECS data, must complete annual CIPSEA training; and have an HHS background check at or above the level needed for the federal government building pass and computer access card. Such training constitutes: online training modules, provided by EIA, on the appropriate handling and use of the PII (such modules appear at <http://www.eia.gov/cipsea/cipsea.html>); and information, provided by ACF, about the existence of the CIPSEA agreement and the penalties for violation.

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.

The CIPSEA agreement describes the processes and guidelines that cover the retention and destruction of all the PII, regardless of source. Such processes and guidelines call for ACF to retain the PII until the sooner of the date on which the subsequent update of the 2015 RECS portion of the data becomes available; or access to such PII is no longer necessary.

ACF returns to EIA or destroys the 2015 RECS data when it no longer needs such data; or when the CIPSEA agreement is terminated. It does so by electronic deletion, shredding, burning, or other approved disposal method. Furthermore, the contractor destroys the PII after the merge takes place. It expects to carry out such destruction within one year after it obtains the data that contains the PII.

OCS is in communications with the ACF Records Manager to determine the retention schedule or schedules required by the National Archives and Records Administration (NARA). All records will be retained until a determination is made as to the final such disposition schedule. After such schedule is established, the records will be disposed in a fashion that's consistent with such schedule.

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

OCS direct contractor, APPRISE, will use only a laptop owned and provided by the agency. It will access the data by connecting such laptop to an ACF Virtual Private Network (VPN) and then using ACF provided credentials to access the Stata Data server on Amazon Web Services (AWS). AWS and VPN are already covered by the agency's security procedures.

APPRISE also has physical controls, including locked cabinets and a secure building, to store the government-furnished equipment (i. e., the laptop) that will be used to access the 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). Additional administrative, technical, and physical controls include: System Access via ACF Personal identity Verification (PIV) badges only; Virtual Private Networks (VPN); System Access via ITIO government funded equipment (GFE) only; Full Disk Encryption (FDE); and TIO GFE that are stored in locked cabinets at APPRISE's facility when not in use.

APPRISE's facility is locked at the end of each business day.