US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2026

OPDIV:

ACF

Name:

LIHEAP Performance Management Website (PMW)

PIA Unique Identifier:

P-1904174-064469

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.

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.

Since the last approved PIA, the National Center for Appropriate Technology (NCAT) has adopted a Microsoft hybrid environment to enhance scalability, resilience, and centralized management across its infrastructure. This transition integrates on-premises resources with Microsoft cloud-based services. NCAT serves as the subcontractor responsible for supporting the environment and security boundary for the Low Income Home Energy Assistance Program Performance Management Website (LIHEAP PMW). There have been no changes to the privacy data elements processed by the system.

Describe the purpose of the system.

The LIHEAP PMW serves as a repository for LIHEAP grant recipient performance management information and other relevant data. The system supports the Department of Health and Human Services (DHHS) in meeting statutory and regulatory reporting requirements from Section 2610 of the Low-Income Home Energy Assistance Act, including information on home energy consumption,

home heating fuels, household income and vulnerable population status. In accordance with the 1994 LIHEAP reauthorization, the Department of Health and Human Services (HHS) is charged with developing performance goals and measures in consultation with grant recipients for assessing their success in achieving the program purpose. The system serves as a repository for LIHEAP performance data from 2001 to the most recent fiscal year. Most of the system data is accessible to the public. Information related to the LIHEAP Performance Management Implementation Work Group (PMIWG) is accessible only to member grant recipients, Office of Community Services (OCS) contractors, and OCS staff.

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

The primary data stored and shared in the system is information from required grant recipient reports, including the LIHEAP Household Report (number and types of households served by LIHEAP) and the LIHEAP Performance Data Form (sources and uses of grant recipient funds, as well as grant recipient performance data). The data from these grant recipient reports are part of the public record on LIHEAP and are included in the LIHEAP Report to Congress.

The other type of information stored and shared in the system is summary information about the performance of individual state LIHEAP grant recipients for each fiscal year. That summary information is developed by the contractor using the primary data reported by grant recipients, information available from the American Community Survey (ACS), and other publicly available data. The summary information is developed according to specifications developed by the PMIWG grant recipients and approved by OCS.

In addition to those data resources, grant recipient performance management training and technical assistance resources also are posted on the website.

Most of the components of the LIHEAP PMW system are accessible to the general public. However, certain components are accessible only to HHS staff, HHS contractors, and LIHEAP grant recipients. To receive a username and password to access the restricted parts of the website, an individual must furnish name, email address, and mobile phone number. That information is stored in a location that is accessible only to the System Administrator. Please note that HHS staff and HHS contractors need to have a username and password to access the restricted parts of the system. They cannot directly access the system with their HHS user credentials. The LIHEAP PMW is an external system and is not part of HHS’s internal environment. HHS staff cannot use their HHS credentials to access the LIHEAP PMW’s restricted areas; instead, they are issued LIHEAP PMW-specific usernames and passwords. User credential information is managed by the System Administrator and stored in an encrypted MariaDB database.

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

The LIHEAP PMW stores data which grant recipients are required to report through the LIHEAP Household Report and LIHEAP Performance Data Form and combines this with publicly available survey data from ACS to give users the ability to analyze and compare LIHEAP performance metrics across multiple years at the state, regional, and national levels.

The data provided in grant recipient reports to LIHEAP PMW from 2001 to 2013 was previously submitted by states directly to OCS and stored on the OCS website. In 2013, this data was imported to LIHEAP PMW. Since 2014, grant recipients have been able to submit their reports through the HHS On-Line Data Collection system (OLDC), which are then extracted, validated for data quality issues, and then uploaded to LIHEAP PMW. Grant recipient data is reported in the annual LIHEAP Reports to Congress, which are also available to view in LIHEAP PMW and can be exported. There are no user restrictions on exporting this type of data.

Data from ACS is obtained using the latest available statistics from the Unites States Census Bureau. The ACS releases publicly available data sets that can be used to generate customized statistics for population groups of interest. OCS personnel use the data to generate counts of income-eligible populations and then upload those counts into the LIHEAP PMW on an annual basis when a new year of data is available from the ACS. LIHEAP also stores and shares LIHEAP performance management technical assistance documents. These documents are created by OCS staff, contractors, or grant recipients.

Publicly available information on LIHIEAP PMW includes published LIHEAP Reports to Congress, a Performance Measures resources webpage, a dashboard of grant recipient progress in reporting LIHEAP Performance Measures, and additional links and content related to LIHEAP performance management such as recent grant recipient report training webinars and training materials on the use of performance management data.

Role-restricted information that is not publicly available includes materials related to LIHEAP Performance Measures and information on the LIHEAP PMIWG, which is only available to participating grant recipients, OCS staff, and technical contractors. PMIWG information meeting materials document the discussion and decisions made during monthly PMIWG meetings.

The data within LIHEAP is officially stored in a separate system OLDC which is part of the GrantSolutions system. The GrantSolutions system has its own records schedule, N1-292-09-1. Items displayed on the Performance Management website include a duplicate copy of the LIHEAP Report to Congress which is covered by the records schedule DAA-0292-2016-0014.

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

Yes

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

Name
E-Mail Address
Phone Numbers
User Credentials - User name and Password

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose of the Personally Identifiable Information (PII) in the LIHEAP PMW is to establish and manage user accounts for role-restricted access to site content.

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

PII in the LIHEAP PMW also is used to furnish business contact information for LIHEAP PMIWG members.

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

Section 2610 of the Low Income Home Energy Assistance Act and HHS regulations for the LIHEAP block grant, cited as 45 C.F.R. Subpart H.

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within the OPDIV

Other HHS OPDIV

State/Local/Tribal

Other Federal Entities

Identify the OMB information collection approval number and expiration date

OMB No. 0970-0060, expires 3/31/2026

OMB No. 0970-0449, expires 6/30/2028

Is the PII shared with other organizations?

No

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

Users are notified that their personal information will be collected during the account creation process. Users receive the following notification prior to submitting their account creation request:

"By submitting a request to create an account, you are consenting to the collection of personally identifiable information (PII). We do not collect PII unless you choose to provide that information to us. Any personal information you choose to provide is protected by security practices. ACF does not plan to disclose, give, sell, or transfer any PII about our registered users unless required by law enforcement or Federal Law."

PMIWG members are directly asked to furnish their personal information and are aware that it is being collected and how it will be used.

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.

PMIWG members cannot opt-out of collection of their PII. Furnishing PII to facilitate communication and networking is a condition of participating in the PMIWG.

Collection of PII for other registered users is voluntary. However, if they do not furnish PII, they will not be allowed to become a registered user.

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

Whenever there is a major system update, notices are emailed to all registered users regarding the update.

Notices will not be sent to public users since their information is not collected and stored.

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.

Registered users can contact the System Administrator using the “Help” function to submit questions and raise any concerns about inappropriate disclosure of PII. The System Administrator will directly respond to concerned users and resolve any issues that they report.

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

Data integrity is maintained by limiting approval and deletion of system accounts to the System Administrator when approved by the System Owner.

Data availability is maintained by daily back-ups of website content.

Data accuracy is maintained by the System Administrator review of PII during account creation, and through periodic review of the website for PII content.

Data relevancy is maintained by reviewing inactive user accounts annually and any users that have been inactive for 180 days or more will be contacted to see if access is still required and deleted if applicable.

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.

Only the System Owner and the System Administrator will have access to the PII collected during account creation.

OCS staff, PMIWG grant recipients, and indirect contractor staff can access PII for all participants in the PMIWG.

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.

Only the System Owner and the System Administrator can access the registered user PII. Public users and other registered users are blocked from accessing the register user PII data.

With the exception of OCS staff, PMIWG grant recipients, and contractors, registered users do not have access to the PMIWG tab of the website and thereby are blocked from access to those PII data.

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.

All internal users (Federal Staff and Direct) of LIHEAP PMW are required to review and sign the acknowledgment of the HHS Rules of Behavior (RoB). This acknowledgment must be completed as part of the annually required HHS Cybersecurity Awareness Training.

PMIWG members receive training on security awareness annually during on-site work group meetings. The PMIWG consists of LIHEAP grant recipients who volunteer to work on development of performance measures training and technical assistance with the support of the contractor team. APPRISE team staff facilitate and document the on-site meetings. OCS staff participate in all meetings.

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

No additional training is provided

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.

We consulted with our office records management liaison, who advised we are initiating a new records schedule for the OCS websites, including this website and the LIHEAP Clearinghouse. The content on the website falls under five different existing records schedules. Those content and schedules include: (1) grant recipient reported data (DAA-GRS-2013-0008-0001); (2) duplicate, courtesy copies of the LIHEAP Report to Congress (DAA-0292-2016-0014-002); (3) limited user information and credentials (DAA-GRS2013-00060003 and DAA-GRS2013-00060004); and (4) technical assistance documents developed by federal and contractor teams (DAA-GRS-2013-0008-0007).

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

Administrative:

Only the System Owner and System Administrator will have access to user account PII information stored in the system. The Administrator receives e-mail notification when a user requests account creation and verifies with the System Owner prior to approving account creation and assignment of user role. PMIWG contact information is made available to users with the user role "PMIWG Grant Recipient". Contact information is reviewed periodically and immediately updated upon notification of a change in contact information.

Technical:

NCAT secures its hybrid Microsoft infrastructure with a SonicWall firewall, integrated monitoring from Defender for Cloud, and Secure Shell (SSH) access restricted to Virtual Private Network (VPN)-authorized users managed via Entra ID. File Transfer Protocol (FTP) port 21 is disabled, and authentication relies on Entra ID. Core code changes are tracked using audit logging tools like GitHub, and monthly penetration tests help identify vulnerabilities. Personally Identifiable Information (PII) is safeguarded through strict access controls and encryption managed with Azure Key Vault in compliance with the National Institute of Standards and Technology (NIST) standards. The Content Management System login forms will be locked down by limiting login attempts to five after which a 120-minute lockout will occur. Two-factor authentication will be used to ensure proper authentication of registered users seeking access to secured PII data.

Physical:

NCAT hosts all its websites at the Thornton Technology and Enterprise Data Center in Butte, Montana, which serves as the core of its Microsoft Hybrid infrastructure. Physical access to the facility is tightly controlled with secure keycard authentication, and NCAT maintains a dedicated fiber-optic link for direct, high-speed connectivity. Within this hybrid model, on-premises servers at

Thornton Labs are integrated with Microsoft Azure services to extend resilience, scalability, and centralized security. The data center’s core network operates over a fiber backbone and is supported by fully redundant power systems, advanced fire suppression, and Faraday shielding to mitigate electromagnetic threats. Hybrid capabilities enable NCAT to enforce cloud-integrated security policies.

Identify the publicly-available URL:

https://liheappm.acf.gov/

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