US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2026

OPDIV:

CMS

Name:

Find Local Help

PIA Unique Identifier:

P-1023324-778844

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?

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.

The Find Local Help (FLH) system has no new changes. The FLH Authority to Operate (ATO) has been renewed as of 9/11/2024 for three years.

Describe the purpose of the system.

Find Local Help (FLH) supports the public search capability of Healthcare.gov web content. The purpose of FLH is to allow the public to locate health insurance resources in their locality/state.

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

Login credentials for applications are stored in application databases. Login credentials for local access to back-end systems are stored on the back-end systems. This includes usernames and password hashes.

Public users do not need to authenticate FLH to view Agent/Broker and Assister information.

Assisters do not authenticate into the system to add/remove/update information via the Assister Landing Page {https://localhelp.healthcare.gov/update-organization-information/#]

Agents/Brokers information is collected externally from FLH and is delivered to FLH by an external source, Marketplace Learning Management System (MLMS).

Login credentials for applications are stored in application databases. login credentials for local access to backend systems are stored on the backend systems. This includes usernames and password hashes.
The FLH page of healthcare.gov provides publicly available health insurance and navigator business contact information. Some data collected by the system is publicly available. The data that is publicly available includes the business names, business email address, business location addresses and the latitude and longitude coordinates of those businesses. The latitude and longitude coordinates aid the search tool in searching within the radius of an address. FLH also collects Personal Identifiable Information (PII) from public consumers such as first and last name, email addresses and phone numbers.
Third-party analytics tools used by the site also collect non-PII information including system performance metrics, and website usage statistics. They are covered by their own Department of Health and Human Services (HHS) CMS PIA or Third-Party Web Assessments (TPWAs):

New Relic
Chartbeat
Adobe Analytics/Mixpanel
Tealium
Twitter (X)
Facebook

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

The Find Local Help (FLH) is a tool, available to the public as a link (https://localhelp.healthcare.gov/) on HealthCare.gov, which allows people seeking health insurance to search for health insurance resources within a locality. Additionally, health insurance resource providers and insurance carriers can submit an online form to request and update publicly available records through a link on the Healthcare.gov website.
FLH data flows as follows: A provider requests changes/updates to resource information. A CMS administrator is alerted and reviews the requests for accuracy. A second CMS administrator approves the request, which results in the data moving into a database along with geo-coordinates provided by MapBox. When a public consumer searches for the data to find local health insurance resources, they access the health insurance information. System administrators, who are also users of the system, can use OpenVPN to access local accounts on the Linux servers to configure the application servers or the databases which are part of the system. In both cases the system administrators must use multi-factor authentication. Login credentials for local access to backend systems are stored on the backend systems. This includes usernames and password hashes.
Some data collected by the system is publicly available. This data includes the business names, business email addresses and business addresses and the latitude and longitude coordinates of those businesses. The latitude and longitude coordinates aid the search tool in searching within the radius of an address. FLH also collects PII from public consumers such as first and last name, email addresses and phone numbers.
Third-Party analytics tools used by the system also collect information and are covered by their own HHS PIAs which can be found at: http://www.hhs.gov/pia/index.html#Third-Party.
The List of tools used by FLH and covered by HHS PIA include:

New Relic - webserver and database performance statistics

Chartbeat - website performance statistics including hits to pages and time spent on pages

Adobe Analytics/Mixpanel - website performance statistics including hits to pages and time spent on pages

Tealium - website performance statistics including hits to pages and time spent on pages

Twitter (X) - a link only

Facebook - a link only

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
Login credentials (user ID and password). Only organizational PII used for login credentials are collected.

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Usernames and passwords are used by System Administrators to access backend systems (servers) of the FLH system.

Consumers - To contact public consumers of FLH if there is any question about information submitted to the application for correction.

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.

The Affordable Healthcare Act, Section 1411

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.

SORN 09-70-0560, Health Insurance Exchange (HIX) Program

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

- Online
- Other

Government Sources

- Within OpDiv

Non-Governmental Sources

- Private Sector

Identify the OMB information collection approval number and expiration date

N/A for user credential information collection.

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.

There is a privacy notice available on the Healthcare.gov website available as a link for consumers to read about the collection and uses of their data.

No prior notice is given by the FLH application itself.

CMS employee and contractor credentials are stored in the system. The expectation of credentials being saved by CMS systems is inherent to employment. Employees do not have an expectation of User IDs remaining private from within the organization.

The individual requesting access to FLH contacts their CMS component`s, CMS Access Administrator (CAA) via email, providing the CAA with their Name, User ID, and email address. The CAA, in turn, enters the data into the Enterprise User Administration (EUA) system, requesting approval for access to the appropriate user job code. This action initiates an email to the FLH System Administrator (SA), requesting his/her approval in EUA. Upon approval, EUA notifies the individuals that their request has been granted. HHS Form 745, ID badge request form, notifies the individual that their personal information will be collected.

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.

An option for users to opt-out of having their login credentials stored within applications or on local systems they access is not available because it is fundamental to the function of the system.

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

Username and password information used for local access (operating system level).   Changes to FLH do not affect the use of this information and System Administrators are not informed about changes to the system relevant to their credentials.   System Administrators do not have the opportunity to consent to system changes.

Health Insurance providers who provided contact information are not informed about changes to the system and are not given an opportunity to consent to changes to the system.

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.

CMS employee and contractor information is stored in the system along with consumer personal information. For CMS employees and contractors, the expectation of names and company e-mail addresses being saved by CMS systems is inherent to employment. Employees do not have an expectation of this information remaining private within the organization.
The information used by tools that are part of the FLH system receives this information from the CMS Enterprise User Administration (EUA) system. If the information (name and company e-mail) is inaccurate, then a simple e-mail to the CMS Access Authority (CAA) with the details of the change would be sufficient to correct the problem and amend the record within EUA.

Consumers who are associated with businesses that have their public information available on the application can submit PII in the form of their first and last names, email address and phone number to be contacted in case of questions about corrections to information submitted.

If an employee or a consumer has a reason to believe that their personal information has been compromised, they can create a ticket with the CMS IT Service Desk at 1 -800-562-1963, which would inform the CMS Cyber Awareness Information Center (CCIC), who would investigate the matter and respond.

In addition, the login credentials, name and email address within this system are collected by Enterprise User Administration (EUA). The EUA PIA describes 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. Individual`s concerns involving their PII (user credentials) are addressed by the Enterprise Administration User team (a function of the contractor, Lockheed Martin).

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

CMS IDs which are used as usernames for local access are created by the Enterprise User Administration (EUA) system. The information was initially entered into EUA via a request form, for the sake of receiving access to CMS system. The form must be approved by the employee’s manager and contracting officer's representative (COR). The EUA system automatically requires users to review their access information annually or they are locked out of all CMS systems. Further, when an employee or contractor is terminated, their access to CMS systems is terminated and their EUA information is deleted.

Passwords (Public Keys) which pair with the username mentioned above, for access to local systems, are created by the user and are verified by the user when they attempt to access the system. If a user is denied access, they can create a JIRA ticket and re-request access and provide a new Public Key to be placed on the target system.

Heath insurance provider business contact information, which FLH provides the public, is initially provided by the health insurance providers through a public interface of FLH. Before the information is consumed by FLH, it is reviewed by CMS for accuracy and relevancy through an FLH interface which is internal to CMS. After the information has been added to the FLH database, it is up to the Health Insurance provider to provide updates through a Public FLH interface. Once the updated information is submitted, two CMS reviewers must review the data in the Admin Interface queue. Once it is reviewed and determined to be accurate, the data is entered into the FLH database.

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 FLH systems is provided through EUA. Prospective users must request a CMS ID through a request form, which must be approved by the employee's manager and COR. After the CMS ID is received, the individual would request entitlement (job codes) through the EUA system. Entitlement requests for User or Administrator roles for various tools are directed to the System Owners for approval.

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.

All FLH tools and local systems maintain User and Administrator roles, which limit access within each application or system.

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.

Both CMS employees and direct contractor staff who access or operate a CMS system are required to complete the annual CMS Security Awareness training provided annually as Computer-Based Training (CBT) course. Direct contractors also complete their annual corporate security training. This training addresses the proper handling of PII.

CMS employees and direct contractors with privileged access are required to complete the annual role-based training and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS are available apart from the regular annual training.

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

FLH employees participate in twice-yearly "Game Day" Exercises," where incident response is practiced and documented. Additionally, ad Hoc provides basic level annual security training taught by security officers within the company.

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 retention and destruction of FLH data is governed by the CMS Records Schedule. This schedule is aligned with the National Archives and Records Administration (NARA) guidelines for data retention and destruction. The following CMS Records Schedule Items apply:

https://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/index.html

Enrollment Records
Disposition Authority Number: DAA-0440-2015-0006-0001
Cutoff Instruction: Cutoff at the end of the calendar year.
Retention Period: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.

Beneficiary Records
Disposition Authority Number: DAA-0440-2015-0007-0001

Cutoff Instruction: Cutoff at the end of the calendar year.
Retention Period: Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized.

Provider and Health Plan Records
Disposition Authority Number: DAA-0440-2015-0008-0001
Retention Period: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.

Analytic and Research Files (restricted) Disposition Authority Number DAA-0440-2015-0009-0002
Transfer to the National Archives for Accessioning: 20 years after cutoff.

Research and Program Analysis: Supporting Records
Disposition Authority Number: DAA-0440-2015-0009-0003
Cutoff Instruction: Cutoff at the end of the calendar year.
Retention Period: Destroy 10 year(s) after cutoff or when no longer needed for agency business, whichever is later.

In addition, the FLH application follows the Data Destruction Standards prescribed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88.

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

FLH has a public interface with no login required. FLH also has an internal interface for Reviewers and Approvers of requests by Insurance providers to add contact information. Access to the internal network must receive approval though the EUA system and credentials are stored in the CMS Lightweight Directory Access Protocol (LDAP) and not on the FLH system. This is role-based access control. FLH backend systems require that individuals who have received role-based training and have a need-to-know may request access to these systems through a JIRA ticket.

System Administrators can access backend systems within the Amazon Web Services (AWS) environment using OpenVPN which requires two-factor authentication. After connecting to an internal Gateway into the environment over the virtual private network (VPN), they are required to have a cryptographic private key on their client system which matches a public key present on the target system. This allows a Secure Shell (SSH) session to be created using which implements Federal Information Processing Standard (FIPS) 140-2 compliant encryption.

FLH physical infrastructure exists in the Federal Risk and Authorization Management Program (FEDRAMP) accredited AWS east region and inherits its physical and administrative security controls regarding system infrastructure. AWS data centers and physical servers are only accessible to authorized personnel. The Office of Communications AWS Cloud Team authorizes remote access to FLH servers.

Identify the publicly-available URL:

https://localhelp.healthcare.gov/#/

This link is part of healthcare.gov and takes public users to the FLH system
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?

No

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