The purpose of the Assister Help Resource Center Support System (AHRCSS) is to provide assistance to consumers enrolling in the Federally Facilitated Marketplaces (FFM) on healthcare.gov. The AHRCSS is comprised of two services, the Enrollment Assistance Program (EAP) and the Assister Help Resource Center Service Desk (AHRC).

The EAP provides consumers with in-person assistance to complete the steps needed to find, choose, and enroll in an appropriate Qualified Health Plan (QHP) for themselves and their family members. The AHRC is a call center to provide expert assistance to the EAP in-person assisters to utilize when they have questions or issues from consumers that they either cannot answer or need more information to assist the consumer.

Describe the type of information the system will collect, maintain (store), or share.
The EAP in-person assisters collect full names, phone numbers, birth year (only), and zip code from consumers and input into the database. The AHRC agents enter call information: name of in-person assister, the purpose of the call, the city and state; and the “knowledge base” information used to provide answers to questions. This information consists of rules, policies, procedures and information about the FFM. For AHRC, the information stored is about in-person assisters who call AHRC, not about consumers the in-person assisters are helping. The system also stores audio recordings of calls received by AHRC.

AHRCSS stores user information about EAP and AHRC staff who access the system, including first and last name, email address, username, and password.

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

AHRCSS is a support service to the FFM health plan enrollment process and provides two service functions; the EAP which assists consumers with questions and concerns about the healthcare enrollment process and the other; AHRC, provides support to those EAP in-person assisters by providing additional information to questions that consumers may have and the in-person assister cannot answer.

Both services utilize the AHRCSS customer relationship management (CRM) database to provide consistent and effective consumer support. The EAP in-person assisters use the CRM platform to record details of their interactions with consumers. This enables EAP management personnel to oversee enrollment assistance operations at the individual staff, site, or program-wide level. It provides consumers continuity of service, so that if an individual interacts with the EAP on more than one occasion, any staff member will be able to assist the consumer with consistent continuity of information and service. The information that the in-person assisters input includes consumer contact information; their full name, phone number, zip code and birth year. This information is used to keep track of information on prior interactions/meetings with the consumer; identify what stage the consumer is in with regard to the application and enrollment process, and report the outcome of the process, once completed.

The AHRC utilizes the database for case management; to track incoming calls and their resolution, and escalate issues internally. The data collected by AHRC will include call reason, caller information (Assister organization, location), audio recordings of calls between AHRC agents and the EAP in-person assisters; and any referrals or escalations that are made. If internal escalations are needed, it will be necessary to collect enough information for the agent receiving the escalation to do the necessary research and follow up.

AHRCSS stores user identification about EAP and AHRC staff who access the system. This user information includes first and last name, email address, username, and password. It also maintains system support staff user credentials, user ID and password.

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

Indicate the type of PII that the system will collect or maintain.
Name
Biometric Identifiers
E-Mail Address
Phone Numbers
Other: Zip code, city and state, year of birth, usernames, passwords

Indicate the categories of individuals about whom PII is collected, maintained or shared.
- Public Citizens
- Vendor/Suppliers/Contractors

How many individuals' PII is in the system?
10,000-49,999

For what primary purpose is the PII used?
PII is used to keep a record of individuals seeking or receiving assistance from project staff, in particular so that a consumer that has multiple interactions can be assisted effectively. PII about assisters contacting AHRC is used to record and track types of support issues encountered by assister/navigator programs in different states to help the government understand what types of issues are being encountered and to facilitate providing expert assistance to in-person assisters. PII about system users (e.g. usernames) is used to enable identification and authentication of users logging in and to provide notification (via email) when new knowledge base articles or other content is available to users in the system.

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.
Patient Protection and Affordable Care Act (Public Law No. 111–148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111–152) Affordable Care Act. Title 42 U.S.C. sections 18031, 18041, 18081-18083 and section 1414.

5 USC Section 301, Departmental Regulations

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 used to cover the system or identify if a SORN is being developed.
- February 6, 2013, and updated May 29, 2013 and October 23, 2013
- Published: CMS Health Insurance Exchanges System (HIX), CMS System No. 09-70-0560,

Identify the sources of PII in the system.
- Directly from an individual about whom the information pertains
  - In-Person
  - Online
  - Other
- Government Sources
  - Within OpDiv
Other

Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date
CMS Form Number: CMS-10400
Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges
OMB control number: 0938-1191
Expiration Date: 05/31/2016

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.
In-person assisters explain the collection of personal information to consumers seeking assistance and all consumers execute a consent form before PII is collected or stored in the system. For the 2015-16 Open Enrollment period, all consumers are provided a written privacy notice explaining what information will be collected, why it will be collected, how it will be used, when and how consent is obtained, how the data will be secured, what privacy rights consumers have regarding their data, and how to file a complaint.

Information on AHRCSS users (first and last names, email addresses, usernames and passwords) is collected at time of hire or at time of assignment to the projects AHRCSS supports. First and last names are furnished by users (employees) at the time of application for employment. Email addresses, usernames, and passwords are assigned to users once they are hired to work on the project.

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.
There is no requirement for consumers to provide personal information to receive assistance. Consumers are notified, verbally and in writing, that "Providing information to us is entirely voluntary; you are not required to provide any information and your choice to provide or not to provide information will not affect your eligibility for health insurance coverage. Our personnel will not deny information or assistance to anyone that chooses not to consent to collection, use, or disclosure of his or her information."

AHRCSS users cannot opt out of providing their names, email addresses, and usernames as these data are required in order to provision user accounts needed to access the system.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
In-person assisters explain, verbally and in writing, the collection of personal information to consumers seeking assistance and all consumers execute a consent form before PII is collected or stored in the system. The contents of the privacy notice and consent form are reviewed and revised as necessary prior to each Open Enrollment season. If significant changes occur to the system or disclosure or use of PII collected from individuals, the affirmative consent obtained from consumers would need to be obtained again. In such a case, in-person assisters would use the contact information maintained in the system to notify users and, if applicable, obtain their consent again.

If there was a major change to the AHRCSS system, the AHRCSS users (in all positions) would be notified by updated training, email notifications and an informational banner at log-in.
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.

Consumers are provided a written privacy notice that includes information about filing a complaint regarding the collection, use, or handling of their information, with contact information for both the CMS Privacy Office and EAP Program Management. Any complaints received are reviewed by CMS and EAP program personnel to determine if any inappropriate action has occurred and, if so, what actions are warranted to resolve the problem.

If AHRCSS users find inaccuracies in their names, email addresses, or usernames maintained in AHRCSS they can request a change or correction to this information from the AHRCSS user administrator.

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

Periodic reviews of information contained in the system, including PII, are performed at regularly scheduled intervals and at milestone dates such as the end of open enrollment. Multiple data integrity protection measures are in place for PII stored within AHRCSS, including change control procedures, system backup, intrusion detection, and anti-virus and anti-malware scanning. Availability is maintained by operating the system within a CMS Amazon Web Services virtual private cloud, which provides high capacity and redundant infrastructure and services. Data accuracy is confirmed at the time of collection, when consumers are asked to verify the accuracy of the information they provide to program personnel. Data relevancy is managed and maintained through explicit standard operating procedures specifying what information needs to be collected from consumers (for EAP) or assisters (for AHRC) to ensure proper provision of services by program personnel.

AHRCSS system administrators review user account information for currency and accuracy at least every six months.

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

Users:
Users are EAP in-person assisters and AHRC agents who perform enrollment assistance and help desk functions; they require access to consumer PII in order to provide these services to consumers and assisters.

Administrators:
System and database administrators require access to PII because they maintain the databases where PII is stored and manage user accounts for AHRCSS users.

Contractors:
All AHRCSS users and administrators are contractors, so they require access to PII in the system in order to provide the services associated with the EAP and AHRC contracts.

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

Access to PII in AHRCSS is limited to users (EAP in-person assisters and AHRC agents) and to system administrators who, among other responsibilities, are responsible for maintaining and backing up the database and supporting files for the system. All AHRCSS users and administrators are employees of the contractor that operates the system. These individuals must pass a thorough background investigation as a condition of hire, so no users or administrators can access AHRCSS or the PII it contains until they have been successfully screened for employment. AHRCSS requires authentication (i.e., login) and authorization (i.e., specific permissions granted to each user) in order to access PII. All user roles and authorizations for the system are documented in the AHRCSS System Security Plan (SSP). Access to PII requires authentication to AHRCSS and authorization (using the role-based access control in the software applications that AHRCSS implements).
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.

User and administrator permissions (authorizations) to access PII are managed through the assignment of roles managed in each software application that AHRCSS implements. Different types of users are assigned different roles (corresponding to different access permissions) by system administrators based on job requirements specified by the project team for different types of users. Within AHRCSS, users are assigned different roles corresponding to different levels of access to data as well as the ability to perform specific actions (e.g., read, update, delete) on that 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 AHRCSS personnel undergo corporate and project-specific training at time of hire and annually thereafter. This training includes security and privacy awareness training with content specific to the protection of PII and protected health information (PHI) and other sensitive or confidential information. AHRCSS personnel also must complete project-specific training provided by CMS before starting work on the project or receiving access to AHRCSS. All personnel must sign agreements to acknowledge awareness of their responsibilities to protect sensitive information.

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

AHRCSS users receive program-specific training in addition to the mandatory security and privacy awareness training given to all employees. This includes CMS-provided training for in-person assisters that must be successfully completed before staff are certified to assist consumers.

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.

PII within AHRCSS records is maintained only as long as needed to support reconciliation or resolution of cases, or to satisfy retention policies established for the FFM. Records management adheres to CMS standards and procedures and to National Archives and Records Administration (NARA) General Records Schedules: 4.1 Records Management Records, which states that records will be retained for a minimum of six (6) years; 4.3 Input Records, Output Records, and Electronic Copies, which states that records should be destroyed as soon as they are incorporated into a master file or longer if needed for business use.

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

AHRCSS implements all security and privacy controls and enhancements specified in the CMS Minimum Security Requirements for a moderate-impact level system. All controls are fully documented the AHRCSS System Security Plan (SSP).

Administrative controls implemented for AHRCSS include access control such as passwords so that only authorized users can access the system, role-based access for registered users, and maintaining audit logs of users activities within AHRCSS.

Technical controls implemented for AHRCSS include firewalls, anti-virus and intrusion detection tools, vulnerability scanning, and encryption of data in transit.

AHRCSS is located within a CMS-authorized data center environment. Physical controls implemented include locked doors requiring access cards for entry, video cameras, and security guards that monitor building access and activity.