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?
   No

Identify the operator.
   Contractor

Is this a new or existing system?
   New

Does the system have Security Authorization (SA)?
   Yes

Describe the purpose of the system.
The Small Business Health Options Program (SHOP) Marketplace was established, as part of the Affordable Care Act (ACA), to allow small businesses to offer affordable healthcare insurance to their employees.

The SHOP Premium Aggregation Service (SHOP PAS) is a subsystem to the SHOP Marketplace. It manages the insurance premium payments from small business employers and the payments to the Qualified Health Plans (QHP).

Specifically, the SHOP PAS provides each participating small business employer with a monthly invoice that identifies the total amount due to the QHP issuers (including both employer contributions and employee withholding contributions). Upon invoice payment, these funds are aggregated from all employers and distributed to the appropriate QHP.

Describe the type of information the system will collect, maintain (store), or share.
SHOP PAS uses the following information in the premium payment process: the small business name, address, email address, telephone, federal tax ID, employer identification number (EIN) and contact person; financial account information; the healthcare plan being offered to employees; the healthcare insurance issuer name, address, telephone and contact.

PAS has access to the small businesses’ employees information, after it is input into the SHOP portal: employee name, date of birth, personal mailing address, personal phone number, personal E-mail address, employment status, social security number (SSN) (optional), dependent(s) information (if any).

In addition to the SHOP PAS account users, there are CMS employees and contractors that support the PAS and will log into the system with user credentials (user ID and password) to provide support functions.

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

The SHOP PAS handles premium payments from employers and disperses the funds to Qualified Health Plans (QHPs). The SHOP PAS functions include the following: billing employers on a monthly basis; receiving premium payments from employers; processing payments received from employers; disbursing premium payments to QHPs; reconciling discrepancies in billings and payments; issuing required notices to the small business employer; and providing banking capabilities to support financial and accounting transactions.

Specifically, the SHOP PAS provides each participating small business employer with a monthly invoice that identifies the total amount due to the QHP issuers (including both employer contributions and employee withholding contributions). Upon invoice payment, these funds are aggregated from all employers and distributed to the appropriate QHP.

To accomplish these tasks, the following information is accessed and used: the small business name, address, email address, telephone, federal tax ID, employer Identification number (EIN) and contact person; the healthcare plan being offered to employees, number of full-time employees participating; healthcare insurance issuer name, address, telephone and contact; and the insurance policy number and total premium due to the QHP.

This information is generated and provided to SHOP PAS from Small Business Health Options Program (SHOP) Marketplace, which has its own Privacy Impact Assessment (PIA).

To access SHOP PAS, an individual must log into the SHOP Portal with a user ID and password. User credentials for small business employers and brokers accessing the system are stored in SHOP Portal. Employees of the participating small business cannot access SHOP PAS. The Qualified Health Plan (QHP) issuer information is from the Federally Facilitated Marketplaces (FFM) and accompanying website, Healthcare.gov.

Information in the SHOP PAS system is stored as long as the small business employer participates in the SHOP Marketplace and is updated annually by the small business.

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

Yes

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

- Social Security Number
- Date of Birth
- Name
E-Mail Address
Mailing Address
Phone Numbers
Financial Accounts Info
Employment Status
Taxpayer ID
Other: Employer Identification Number, Member Identification Number, Policy Number, user

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

How many individuals' PII is in the system?
   100,000-999,999

For what primary purpose is the PII used?
The primary purposes for using PII in the SHOP-PAS system is to handle premium payments from employers and disperse funds to issuers; and access to the system by support personnel.

Describe the secondary uses for which the PII will be used.
   Not applicable

Describe the function of the SSN.
   SSNs are used to identify the unique individual insured(s).

Cite the legal authority to use the SSN.
   Per the Affordable Care Act, Section 1411; CMS must collect the SSN for use in determining citizenship and immigration status.

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 sections 1411, 1414.

5 USC Section 301 Governmental 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 use to cover the system or identify if a SORN is being developed.
   Health Insurance Exchange (HIX) Program, 09-70-0560 (February 6, 2013; May 27, 2013 and

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

Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date
Not applicable.

Is the PII shared with other organizations?
Yes

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

Private Sector
PII is shared with QHPs to determine premiums and payment processing. It is also transmitted to financial institutions for payment processing and US Bank for the sharing of the small businesses' financial account information.

Describe any agreements in place that authorizes the information sharing or disclosure.
An Interconnection Security Agreement (ISA) is in place with US Bank authorizing the sharing of the small businesses' financial account information.

An ISA is in place with the Allison Payment System for the mailing of invoices. The contract incorporates a Health Information Portability and Accountability Act (HIPAA) Business Associate Agreement.

Describe the procedures for accounting for disclosures.
There are no disclosures of PII outside of what is permissible, for SHOP PAS to operate. The system accounts for all disclosures by maintaining an audit record of what information is disclosed to the external parties and for what specific purpose.

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 no process in place to notify individuals that their personal information is collected because SHOP PAS does not collect PII directly. The SHOP Marketplace provides notification at the time of account creation and each time an individual logs into SHOP-Portal. The SHOP-Portal has its own PIA.

PAS support System personnel (CMS employees and contractors) access the PAS through the CMS Intranet and are notified at that login point that they are accessing a government system.

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.
Within the SHOP PAS system, there is not an opt-out option because PII is not generated/stored or input into the system. It exists as part of information received from the primary system, SHOP-Portal.

The system's support personnel (administrators, developers) access the PAS through the CMS Intranet and are notified at that login that they are accessing a government system and that there is no option to opt-out if they want to perform their job functions.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
There is no process to notify and obtain consent from individuals about major changes to the system because SHOP PAS does not collect PII directly from the users of 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.**

There is no direct process in place to resolve an individual's concerns of misuse of their PII within SHOP PAS because the PII is collected by the SHOP-Portal.

The system's support personnel (administrators, developers) access the PAS through the CMS Intranet and if they have a concern, they may contact CMS' IT (information technology) Help Desk via email or telephone. The Help Desk would investigate and work with the individual to resolve their concern.

**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 utilizes a National Institute of Standards and Technologies (NIST) compliant continuous monitoring program to ensure system integrity, availability, and confidentiality. As part of CMS, SHOP PAS is included in that monitoring program.

The SHOP individual enrollment application is designed with logic checks to ensure data accuracy and integrity. Yearly, the CMS Center for Consumer Information and Insurance Oversight (CCIIO) is required to review and update the enrollment process to ensure data collected is relevant to the health insurance enrollment process.

SHOP PAS has implemented the following quality checks to ensure the integrity, availability, accuracy and relevancy of the PII contained within it.

The first one is a Data Integrity Quality Assurance (DIQA) report that compares the information in SHOP PAS with the enrollment information in the SHOP-Portal. Each week, PAS receives a DIQA extract from the SHOP-Portal. This extract is compared to the PAS data on employers/members. A Data Analyst reviews any discrepancies and takes action to ensure that they are resolved. Actions include: identification of transaction processing issues, manual corrections required for non-automated personal data transactions, and Help Desk tickets sent to the enrollment system for resolution. Discrepancies are tracked and reported on until all systems are in sync.

The second quality check is "Enrollment Reconciliation." The process involves comparative reporting between SHOP Portal, SHOP PAS and QHPs. Monthly, SHOP PAS receives enrollment files from each of the participating QHPs/issuers. These files are compared to the Enrollment DIQA report from SHOP Portal. A discrepancy report is generated and sent out to each Issuer for the issuer to review. If the issuer believes that the discrepancy is a result of inaccurate data on the SHOP Enrollment system, there is a discrepancy reporting process for them to submit information back to SHOP Portal. Those requests are reviewed/analyzed by a Data Analyst and appropriate action is taken. For example, explanation of the data is sent back to the Issuer and a Help Desk ticket is sent to the Portal/PAS systems and the small business employer is contacted for corrective action.

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

**Administrators:**
System administrators do not specifically access or use PII as part of their system maintenance support activities. However, because they need to have administrator access to perform their maintenance and support activities they may have access to PII.

**Developers:**
System developers do not specifically access or use PII but because of the type of work provided, they may have access to PII by working on the system updates, improvements, changes to the technology.
Contractors:

Contractors have Administrator and Developer roles and do not specifically access or use PII as part of their system maintenance support activities. However, because they need to have administrator access to the perform their maintenance and support activities they may have access to PII.

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

Access is to PII is granted based on the user's role following the principles of minimum necessary and least privilege. Managers must approve all system access and re-certify that access within every 365 days.

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 system employs role based security. Access is always based on least privilege, explicitly denied unless otherwise granted. Access controls limits the ability for administrators, developers, and contractors to access PII. PII data is masked in testing and developer environments.

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.

Security Awareness and Privacy training is required and provided to the system personnel on an annual basis. CMS employees and support contractors with CMS accounts must take the annual Security and Privacy awareness training provided by CMS. Users acknowledge successful training after passing a test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data.

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

Security personnel receive additional job related training by attending conferences, forums, and other specific training on an annual basis. Security based role training is recorded within the contractor's security department.

Contractors implement Security and Privacy Awareness training programs providing general security and privacy awareness training at the time they are hired, before accessing the SHOP PAS system, and annual refresher training thereafter. In addition, periodic reminders are sent via email, as well as items in a weekly contractor newsletter.

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.

In the event that paper documents are received, documents will be destroyed weekly by placing them in the Cintas Document Management bins. Any scanned checks and coupons will be stored for 60 days after deposit in locked cabinets within a secured area with a badging system and security cameras and then destroyed. The weekly destruction of the documents is done by specifically trained staff. The department manager will be responsible for signing a Document Archive and Destruction Log and releasing the work to be destroyed. These procedures are in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration General Records Schedule 20 (GRS 20) for electronic records. DISPOSITION: Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes (Disposition Authority: GRS 20, Item 1).

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.
The SHOP PAS does not store PII and use encrypted communications between the systems that exchange data. SHOP PAS has been evaluated by a third-party assessor that has determined the system meets the Acceptable Risk Standards (ARS) 2.0 as established by the CMS Chief Information Security Officer.

Administrative controls such as written policy, procedures and guidelines have been established. Administrators of the system are vetted prior to hiring and are required to receive annual Security and Privacy awareness training. Third-party assessment validated the implementation of the logical or technical controls that have been implemented to prevent unauthorized access, to safeguard the data in the event of a disaster, and to audit activity within the application.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users access PAS and computer system controls that prevent users without administrative or developer access to log into a test environment and the test environment and usable application are not joined together.

SHOP-PAS is hosted by a qualified Data Center that employs physical controls and monitoring to restrict physical access and ensure the security of doors; the efficacy of heating and air conditioning, smoke and fire alarms, and fire suppression systems; and by employing cameras, fencing and security guards.