US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/29/2016

OPDIV:

CMS

Name:

Health Insurance and Oversight System

PIA Unique Identifier:

P-3906017-027802

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?

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.

A new module has been added to the Health Insurance and Oversight System (HIOS). The Rates & Benefits Information System (RBIS) is no longer a stand-alone system and this system has transitioned to a module within HIOS.

Describe the purpose of the system.

The Health Insurance and Oversight System (HIOS) is a web-based application that allows CMS Center for Consumer Information and Insurance Oversight (CCIIO) to collect insurance statistical data from state entities and individual and small group health insurance carriers (Market Issuers). The information is aggregated with other CMS data sources and made public on a separate, CMS consumer- facing website, www.cms.gov. The information available is in the form of reports, fact sheets and other informational documents.

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

The information collected, stored shared, and retained within HIOS is based on healthcare plan year and is replaced or updated annually.

HIOS PORTAL houses and provides access to each Module. The portal allows system administrators to perform functions such as Manage Account and an Organization to create account, edit information and assign users to access modules.

HIOS PF collects State and Private Market Issuer health insurance information. For State users, PF collects insurance product information (coverage, deductibles, prescription plan) sold to individual and small group participants to compare to the insurance plan filings of those issuers.

RBIS provides Market Issuer users with the capability to submit and manage detailed product benefit and eligibility information about their plan offerings.

CAP is used by states and its case workers. The information submitted includes: types of cases handled by caseworkers, number of individuals per reporting period, and types of issues (coverage denials, enrollment assistance, and appeals of decisions).

MLR data includes: premiums paid to Market Issuer, claims amounts paid, applicable fees, expenses related to resolution of claims. The system also allows users to attest to uploaded data within a defined submission period.

RRJ supports the CCIIO and the States' Departments of Insurance (DOI) ability to review health insurance premium rates to protect consumers from unreasonable rate increases, track all rate changes, and brings visibility to unreasonable rate increases.

RRG collects reports provided by the states, on how they utilize grant funding, metrics regarding rate change data submitted to them by Market Issuers and the States’ review of these rate changes.

HPOES assigns a unique health plan identifier (HPID) and other entity identifier (OEID) numbers to Market Issuer Company. These are not identifiers of individuals. The system facilitates the submission and approval of HPID and OEID applications.

ERE collects information related to the External Review process of appeals health insurance plan decisions concerning denied payments for a service or treatment.

NON-FED allows both self-funded and fully insured health insurance plans to register their organization and elect to exempt those plans from (“opt out of”) 7 provisions of title XXVII of the Public Health Service (PHS) Act.

ASSISTER MODULE allows Assister Organizations to create, edit, attest, and certify assister records. The records contain Assister's name; job title; organization name, address, telephone and email; and Federal Employer Identification Number (FEIN).

CCS allows Market Issuers to complete their certification of compliance submission requirements.

MQM provides score ratings. Users can review/preview ratings and the data will be available for data dissemination to the Analytic platform, and Federal and State Marketplaces, in accordance with the Affordable Care Act (ACA).

DCM leverages existing HIOS data, such as issuer data and product data, to facilitate data entry associated with submission. The system supports the upload of multiple documents from issuers for compliance assessment. This allows web-based data entry based on the minimal number of data elements being collected. Included are the 4 sub-modules as follows:

DCM SDC provides States with the ability to submit the Effective Rate Review Survey via online submission for review by the CCIIO.

DCM MC allows HHS users to create requests to Market Issuers for documentation in support of a Market Conduct Examination (MCE).

DCM FF allows Market Issuers to upload their insurance plan filings of policy forms and program information (deductibles, coverage, prescription benefits) and add supporting documentation to these submissions.

DCM MEC allows users to create submissions on behalf of their organizations, consisting of Certifying Official contact information and any documentation pertaining to their MEC plan(s).

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

HIOS is a web-based application that allows CMS's CCIIO to collect health insurance plan data from state entities and Market Issuers. It is aggregated with other CMS data sources and made public on a separate CMS consumer- facing website, www.cms.gov.The data collected through HIOS is published in various formats like reports, fact sheets and other informational documents.

The entities from which the information is received are the States' DOI, State-based health exchanges and the Market Issuers. Market Issuers are the health insurance providers that offer individual, small or large group plans in the private health insurance market.

HIOS is accessible only after a user account and ID is successfully generated via EIDM where the authentication process occurs, www.portal.cms.gov. The PII that is collected via the EIDM portal is subject to the EDIM PIA P-9873401-033331. After authenticated/authorized by EIDM, a user selects the HIOS application button and inputs their user credentials- user ID and password. These credentials are created and stored within the EIDM system for the length of employment/need to access the HIOS system.

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

Other - User credentials- user ID and password; Job Title, Organization Name, Organization

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

Employees

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

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose for collecting PII is for access to HIOS. Within the Assister module, an individual's business-related PII is used to certify them to provide services to consumers. There is no disclosure of PII outside of the HIOS system.

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

Not applicable

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

Authority for maintenance, collection and disclosures of information is given under sections 2719, 2723, and 2761 of the Public Health Service Act and section 1321(c) of the Affordable Care Act and 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 use to cover the system or identify if a SORN is being developed.

Health Insurance Exchange (HIX) SORN: 09-70-0560, published February 6, 2013 and updated May

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Number 0938-1236. Expiration Date4/30/2017.

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.

HIOS does not directly notify individuals because it is accessed through EIDM. When a user logs into EIDM, there is a Terms and Conditions statement that the user must click the "I Agree" button to move forward. It states that their information is being collected.

Additionally, when someone creates a new user account, there is a "Consent to Monitoring & Collection of Personally-Identifiable Information" introduction displayed on the Terms & Conditions page. The person can elect to "Decline" the Terms and Conditions and then no account will be created.

The users are also provided disclaimer notification once in the HIOS portal which also must be acknowledged by clicking "I agree".

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 isn't an 'option to object,' since the process is voluntary and necessary only if an account creation is desired. The person can elect to "Decline" the Terms and Conditions and then no account will be created.

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

Since the HIOS system is part of the EIDM environment, notification of any major changes to the system related to PII would be done by EIDM, in the form of online notices on portal.CMS.gov. Additionally, the HIX SORN will be updated on the Federal Register.

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.

Within the HIOS portal there is a notice that individuals may contact the Exchange Operations Support Center (XOSC) at a toll free number or at the designated email address, if they have any questions or concerns regarding the use of their PII in HIOS. The XOSC would contact the individual and investigate the concern. If necessary, there might be changes made to the user's access or PII.

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

PII is submitted and managed (including any corrections) by the user. Incorrect data is corrected in the course of using the system by updating whichever element is incorrect, for example, a name change, or new telephone number, email address.

HIOS administrators maintain the allowable/registered users by deleting, reactivating and assigning users to modules. The availability of the user accounts is managed on the back-end by EIDM, since that is where the initial creation of the user account occurs. There are processes in place to review the current users and eliminate any inactive accounts such as user accounts of individuals are removed from the group or automatically disable inactive HIOS accounts within 60 days.

Data integrity and availability is also managed by security technologies, including firewalls and encryption layers.

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

Users:

Users of the Assister module upload PII of the Assisters for certification.

Administrators:

Authorized users such as administrators are provided with a minimum necessary system access for each module for the performance of required tasks. Administrators do not regularly access PII. There are discretionary security controls and audit controls are in place.

Developers:

Developers are provided with a minimum necessary system access. Developers do not regularly access PII but only as necessary to perform tasks. Discretionary security controls and audit controls are in place.

Contractors:

In their roles as either an administrator or developer, a direct contractor may have access to PII to perform those job functions

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

Those with access to PII have only the minimum amount of information necessary to perform their job in accordance with the least privilege principle. There is a process in place for requesting, establishing, issuing, and closing user accounts and tracking access authorizations. The disabling of inactive accounts and auditing of user accounts allow those with access to PII to only access the minimum amount of information necessary to perform their job.

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.

HIOS users are granted the minimum access necessary to perform their job function. There are different levels of access depending on the role of the individual accessing HIOS, in accordance with role based privileges. All HIOS users are authenticated via the EIDM system credentials. If an individual is removed from a module or automatically disabled, then the account is made inactive in HIOS within 60 days. There is also multi-factor authentication of the user for access (two log-in screens). The direct contractor accounts are reviewed annually in order to determine if a user still requires access to the 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 CMS employees and Direct contractors with access to CMS networks, applications, or data must complete mandatory annual Security and Privacy Awareness Training. Since HIOS is a CMS application, the system personnel must take the CMS Security Awareness training. Direct contractors also complete their own annual corporate security training.

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

CMS employees and direct contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role and participate in an annual contingency planning exercise.

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 HIOS system is subject to the HIX SORN which states: These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with published records schedules for CMS, as approved by the National Archives and Records Administration

(NARA).

The CMS Records Schedule notes that HIOS records should be transferred to inactive storage after one year and destroyed after 7 years, unless necessary in the investigation of fraud or overutilization of services. If needed for those scenarios the records are retained until the resolution of the investigation

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

PII is secured in the system using administrative, technical, and physical controls, in accordance with policies and regulations detailed in the CMS Information Security Acceptable Risk Safeguards-Minimum Security Requirements (ARS).

Administrative controls include role-based permissions to access HIOS modules, request and authentication through the CMS EIDM system, and periodic review of users and deletion of non-active accounts.

Technical controls include access is allowable through one of 3 Internet gateways; limitation on the number of concurrent sessions two concurrent sessions, inactivity timeout, multi- factor authentication and intrusion detection and prevention software.

Physical controls include video monitoring of the data center where the system resides; controlled heating, air conditioning, smoke and fire suppression systems; and restricted access with fencing and security guards.

Session Cookies that collect PII.