US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/29/2016

OPDIV:

CMS

Name:

Federally Facilitated Exchange Analysis Tools

PIA Unique Identifier:

P-9594868-634874

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?

No

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Center for Consumer Information and Insurance Oversight (CCIIO) uses the Federally Facilitated Exchange Analysis Tools (FFEAT) system to review health insurance companies' (issuers) applications, rates and benefit packages to become Qualified Health Plans (QHP) and Stand-Alone Dental Plans (SADP) that are offered on the Federally- Facilitated Marketplace (FFM). QHP and SADP are offered to the general public and to small businesses under the provisions of the Affordable Care Act (ACA) on the FFM website, healthcare.gov.

The FFEAT's suite of reporting and analytic tools provide CCIIO with timely ad-hoc analysis and reports and reviews of health plans.

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

The FFEAT system stores information for user access. This includes the individual's full name, business email address, user ID and password.

The FFEAT system stores information that describes health and dental plans. This information includes the issuers, QHP and SADP name and business contact information for corporate representatives, and insurance plan descriptions, rates, plan options
and benefits and operational plans. The information about the issuers, QHP and SADP does not include any information about the general public or individuals insured in any plan.

During the review of insurance and dental plan submissions, reviewers record the outcome of reviews by adding comments, identifying deficiencies and performing supervisory and Quality Assurance (QA) approval. Audit logs are maintained that capture the user, date and time of all system actions to facilitate audit.

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

CCIIO uses FFEAT to perform ad-hoc analysis and prepare high level reports to summarize various aspects of the healthcare marketplace, including: reports that show premiums, benefit package characteristics, and other data elements relative to the product offerings that issuers are offering on the FFM; county coverage maps and reports that indicate full- shelf (or the lack thereof) counties where there is adequate competition of plans in the FFM; year-over-year comparison reports and analyses of what products QHP issuers offered on the FFM; deficiency counts by review area where issuers need to correct or update their QHP applications in order to be in compliance with CMS regulations to be certified to sell QHPs on the FFM.

FFEAT allows the CCIIO to review QHPs and SADPs in order to ensure they are meeting specific benefit and value standards. Types of reviews that are performed include: administrative, compliance plan, licensure, good standing, accreditation, network adequacy, service area, essential health benefits, actuarial value, and cost sharing evaluations. During the review of health and dental plan submissions, reviewers record the outcome of reviews by adding comments, identifying deficiencies and performing supervisory and QA approval. Audit logs are maintained that capture the user, date and time of all system actions to manage and facilitate audits.

The information captured during review is used to provide feedback to issuers. Any deficiencies identified in an issuer's submission are corrected by the issuer. The deficient submission is resubmitted and reviewed again.
After a complete review with no deficiencies and certification by CCIIO, issuer submissions are offered for sale on healthcare.gov/FFM. The FFEAT system stores information that describes health and dental plans. This information includes the issuers, QHP and SADP name and business contact information for corporate representatives, and insurance plan descriptions, rates, plan options and benefits and operational plans.

The FFEAT system stores user information about the FFEAT staff that conduct the reviews and the system support staff that provide administrative services. The user information is full name, email address, 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

E-Mail Address

Other - Password, User ID: This information includes the issuers, QHP and SADP name and

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?

500-4,999

For what primary purpose is the PII used?

The PII is used to authenticate users when they log into FFEAT.

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.

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 Information Exchange (HIX) 09-70-0560 02/06/2013 and updated 5/27/2013 and 10/23/2013

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

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable for user credentials.

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.

Prospective users of FFEAT must sign an account request form. New users receive a welcome email with instructions that includes a notification that their name and business email addresses are maintained for authentication purposes.

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.

Users are notified of the method to opt-out in the new user welcome email.

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

FFEAT users receive regular emails about the system, including notices of changes to the system. User IDs and passwords are never distributed, so system modification will not alter how the information is protected.

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.

If an individual has a concern regarding use of their PII, they are instructed to contact the FFEAT Program Privacy Officer.

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

A user audit is performed on a monthly basis. User audits consist of review of user activity, failed login attempts, inactive users, and password changes are conducted by the FFEAT Information System Security Officer (ISSO). The FFEAT Program Privacy Officer also conducts a monthly audit of PII usage.

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

Administrators:

An administrator has access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Also, administrators conducting monthly audits access system logs that show users ID and time and date of the system access.

Contractors:

Contractors have access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Also, administrators conducting monthly audits access system logs that show users ID and time and date of the system access.

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

Prospective users of FFEAT must sign an account request form. Users and their roles are reviewed and approved by the business owner before access is granted to FFEAT and users are granted access on a "need-to-access" basis for their assigned duties. A user audit is performed on a monthly basis. User audits consist of review of user activity, failed login attempts, inactive users, and password changes are conducted by FFEAT ISSO.

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.

FFEAT uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to- access" commensurate with their assigned duties. A user audit is performed on a monthly basis. User audits consist of review of user activity, failed login attempts, inactive users, and password changes are conducted by FFEAT ISSO. Passwords are obfuscated by design and can only be changed by an administrator.

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 users are required to complete the annual CMS Security and Privacy Awareness training provided annually as Computer Based Training (CBT) course. Any individuals with privileged access must also complete role-based security training commensurate with the position they are working. Contractors also complete their own annual corporate security training.

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

No additional training is required.

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.

FFEAT follows the CMS Records Schedule published April 2015 and the National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 and 24.
Specifically, National Archives Records Association (NARA), General Records Schedule (GRS) 20 states that FFEAT will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later; and GRS 24 states that FFEAT will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

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

FFEAT uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to- access" basis that commensurate with their assigned duties. Users and their roles are reviewed and approved by the business owner before access is granted to FFEAT A user audit is performed on a monthly basis. User audits consist of review of user activity, failed login attempts, inactive users, and password changes are conducted by FFEAT ISSO. The FFEAT Program Privacy Officer also conducts a monthly audit of PII usage.

Encryption is used for all backup tapes and data connections. Additionally, multiple intrusion detection and prevention methodologies are employed, and the system is tested regularly (multiple times a year) for application vulnerabilities, and daily for system vulnerabilities. Access is provided by multi- factor authentication and the system is not publically available.

FFEAT is located in a Tier-1 network data center which provides premier physical control protections. Physical controls are in place such as security guards ensure that access to the buildings is granted to authorize individuals.
Identification of personnel is checked at the data center.