US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2017

OPDIV:

SAMHSA

Name:

BPM

PIA Unique Identifier:

P-3021093-701715

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?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

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 (BPM) Business Process Manager hosts web based workflows on the GSS AWS to support SAMHSA employees andcontractors. AWS stands for Amazon Web Services, which is the FedRamp-certified private cloud hosting environment used by BPM. The internal workflows such as ETHOS, HIRE, Q-Concept, Telework, and (CTAS) Conference Tracking Approval System are allowed through BPM access. HIRE is the name of the application to process and track new employees. Workflow consists of the services (ETHOS, HIRE, Q-Concept, Telework, and (CTAS) in processing information. These workflows are not publically available and they are accessed by internal users only.

ETHOS is an enterprise-wide ethics system which enables government employees to submit financial asset information; HIRE workflow tracks all newly hired government and Commission Corps employees for hiring metrics.

Q-Concept is an enterprise-wide workflow that supports SAMHSA's Communication Planning and Clearance Process; Telework is a workflow that allows employees to submit their telework agreements to be reviewed and approved by
their supervisor.

Conference Tracking Approval System (CTAS) is an enterprise-wide web-based workflow that allows users to enter data regarding their participation in external conferences. Presently there are no separate PIAs for each of these workflows.

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

The BPM will employ five workflows (series of activities that are necessary to complete a task) that will capture various PII data. For that data, three workflows (ETHOS, HIRE, and Telework) will interface to provide tracking for employees. The Q-Concept and CTAS workflows will not capture PII information and will not interface with the other workflows that collect PII data. The current CTAS system consists of a data entry application developed on Microsoft .NET, a record keeping system developed on Microsoft SharePoint, and a paper-based approval process.

CTAS does not capture PII as it only includes data on conferences. ETHOS collects user information (name, work phone number, email, work addresses and references), which is stored in BPM, and uses it for authentication purposes for users logging in for data entry purposes. Additional data elements may be captured arbitrarily on submitted forms such as education records, legal documents and employment status. The information collected by the BPM using ETHOS is an enterprise-wide ethics system which enables government
employees to submit financial asset information, income data, debt data (Self, spouse, and dependent children), financial liabilities, and confidential financial disclosure which can be reviewed by the Ethics Officer and certified by the Ethics Certification Officer. HIRE will store information related to candidate employment application, which may comprise of e-mail address, home address and phone number. HIRE captures education records, Date of Birth, relevant legal documents, and employment status which are needed for hiring purposes. Telework workflow collects and stores home address and telephone number. For each of the workflows that are listed in the BPM application, the approved administrator (direct contractor) will utilize HHS credentials and PIV information.

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

The BPM hosts web based applications to support the SAMHSA employees and contractors. The ETHOS workflow captures PII in order to track ethics outcomes. Request For Approval Outside Activity form (HHS-520) collects employee name, phone number (office, cell, fax), address, email, salary, position, supervisor name, time period, travel cost estimate, compensation (fee, honorarium, stock, royalty, etc), name of funding source and is funder receiving any HHS grant or contract. The form HHS-521 Annual Report Of Outside Activity employee summarizes the results of all filed forms HHS-520. OGE Form 450 collects data only for CONFIDENTIAL FINANCIAL DISCLOSURE REPORT for Executive Branch. employee name, phone number, email, salary, agency and agency address, position, assets and liabilities, and supervisor name, email address, and phone number.

Financial data are used with the purpose to assist employees and their agencies in avoiding conflicts between official duties and private financial interests or affiliations.

HIRE and Telework are used to track employment status and work schedule. HIRE captures education records, Date of
Birth, relevant legal documents, and employment status. This information is uploaded by SAMHSA employees and
contractors, and it contains confidential or personally identifiable information (PII).

Information is stored in an encrypted database and is not publicly accessible. The information is accessed through approval from the BPM application administrator. For each of the BPM workflows, the administrator (who is a direct contractor) utilizes HHS credentials and PIV information to access the system.

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

Yes

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Certificates

Legal Documents

Education Records

Employment Status

HHS Credentials

DOB (documents uploaded to ETHOS may contain this data.)

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

Employees

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary use for the PII in BPM will be to track human resource related initiatives concerning employees. The PII will be used to identify individuals associated within each of the workflows within BPM.

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.

5 USC 301

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.

09-90-0018 (Personnel Records in Operating Offices, HHS/OS/ASPER)

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other

Identify the OMB information collection approval number and expiration date

Not Applicable.

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 each workflow for BPM the individual is provided a form to complete and each form has a privacy act statement notifying individuals to their consent and what responsibility the agency will take in collecting their PII.

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.

For each workflow within BPM there are various levels of opt-in/out methods. For the ETHOS workflow this is strictly voluntary upon receiving training on what constitutes ethical reporting. The employee does have the option to opt-out by not providing their information. The same process follows for Q-Concept, HIRE, CTAS and Telework in terms of opting out of providing some information though it would compromise further processing on HIRE.

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

All the attachments have privacy statements in the forms with consent and disclosure language.

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.

PII entered in the uploaded forms are only viewed by individuals with designated roles in BPM. The submitter of the forms are entering their PII, which by default any inaccuracy could only be updated by the submitter. The administrator has the ability to fix incorrectly submitted information.

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 contained as attachment in the work-flow. To ensure the data's integrity, availability, accuracy and relevancy include the following controls: access control restricting users with Role Based Access, technical controls such as data storage in an encrypted database.

There is not a process in place to ensure the data's
accuracy and relevancy other than by users noting possible discrepancies.

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

Users:

Users are individual who complete and upload their information in the BPM application for each workflow.

Administrators:

Administrators grant access to the program manager. The program manager provides access for the users.

Developers:

Developers need to modify and update applications if required.

Contractors:

Direct contractors require the access to troubleshoot the application and to gain insight into the performance of certain applications.

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

The administrator provide access to the program manager for each of the workflows. Individuals (who may be employees or the developers) are only granted access to the workflow that is relevant to that user's role which restricts access to specified permissions to perform certain functions and access to PII.

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.

Individuals with Role based Access are allowed to review and approve the workflows but are limited by their role based access in terms of what PII can be viewed. These individuals include immediate supervisors, program coordinators, deputy counselors, and Center/Office leadership all others would be denied access.

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.

BPM and awareness training is provided to BPM users and operators. This training also encompasses HHS Privacy and security awareness training.

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

Role Based Access training will be provided to the users from the SAMHSA security team.

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 record schedule is currently being updated by SAMHSA. Once there is an approved record schedule we will update the file accordingly.

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

Administrator grants Role based access to each user.

Administrative controls include proper training by completing HHS Security Awareness training, signing HHS Rules of Behavior and proper on boarding following HHS rules. Technical controls include audit trail, logging, logical access controls restricting access. Other technical controls include data stored in encrypted database, access only through use of HHS computer involving two factor authentication and PIV card. Physical controls include proper on boarding and having PIV card as valid identification.

BPM is hosted in AWS GovCloud, all the physical controls are maintained and secured by the AWS.