US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2025

OPDIV:

NIH

Name:

Employee Assistance Program Case Management System

PIA Unique Identifier:

P-6672739-617035

The subject of this PIA is which of the following?

Minor Application (child)

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?

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.

This validation is intended to refresh content and update the status of Employee Assistance Program Case Management System (EAP CMS).

Describe the purpose of the system.

The National Institutes of Health (NIH) Employee Assistance Program (EAP) is a confidential consultative and support service that assists employees and their immediate family members with personal, family, or workplace mental health concerns impacting well- being and work productivity. The EAP Case Management System (EAP CMS) is a software that maintains and stores records of health information and clinical events related to the EAP services provided to employees, individuals on collateral sources and work groups.

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

The EAP CMS system captures mental health screening data, including substance use screening, as well as needs & risk assessments and counseling related to mental health concerns in clinical

notes. The data elements collected and stored are name, email address, phone numbers, medical/clinical notes, education records, military status, date of birth, mailing address, and employment status.

Users log in to the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

The National Institutes of Health (NIH) Employee Assistance Program (EAP) is a confidential consultative and support service that assists employees and their immediate family members with personal, family, or workplace mental health concerns impacting well- being and work productivity. The EAP Case Management System (EAP CMS) is a software that maintains and stores records of health information and clinical events related to the EAP services provided to employees, individuals on collateral sources and work groups.

The EAP CMS system captures mental health screening data, including substance use screening, as well as needs & risk assessments and counseling related to mental health concerns in clinical notes. The data elements collected and stored are name, email address, phone numbers, medical/clinical notes, education records, military status, date of birth, mailing address, and employment status.

Users log in to the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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
Medical Notes
Education Records
Military Status
Employment Status
Substance use/abuse history
Mental health history

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

Employees
Public Citizens

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Validate and authenticate individuals that seek confidential consultative and support from EAP service.

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

N/A

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

5 U.S.C. 7361, 7362, 7901, 7904; 44 U.S.C. 3101

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.

09-90-0010, Employee Assistance Program (EAP) Records.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

Currently, there is no OMB Clearance. Once the freeze lifts on requesting OMB Clearance, the PIA will be updated with the clearance number and expiration date.

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.

Notification takes place at intake of case management where individuals are verbally informed they are required to provide their information as part of the case management collection process. After this, an email is sent advising the client of the appointment details and forms that must be completed prior to the appointment taking place. After three months, a follow-up is conducted to close the case. If any changes have occurred in the system, the client will be notified during the follow-up.

For EAP CMS users, NIH Enterprise Directory (NED) is the source system for PII. Consent for major changes is handled by NED. NED maintains its own PIA, including all legal authorities.

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.

Individuals may opt-out of the collection or use of their PII by not participating in the EAP. By participating in the EAP, the individual grants explicit consent for the collection and/or use of their PII.

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

A de-identified group email with opt-out language will be sent to all individuals to re-consent.

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.

Individuals may contact their Institute, Center, or Office Privacy Coordinator or the NIH Senior Official for Privacy at privacy@mail.nih.gov.

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

EAP CMS undergoes regular and periodic reviews.

The EAP CMS has annual reviews of PII contained in the system, as well as audits of data logs to assure all information is accurate and relevant.

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

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

Access is granted only to EAP CMS users and approved by NIH management based on their technical/functional role in administering, developing, and supporting the daily job functions of EAP CMS.

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.

Periodic review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of EAP CMS.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

Users with additional roles for system administration, risk management, leadership, continuity of

operations and safety receive additional training for ethics, equal opportunity and diversity, the Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act), and use of strategic sourcing.

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.

Records are retained and disposed of under the authority of the NIH Records Retention schedule Records Schedule System .

General Records Schedule (GRS): Human Resources- Employee Health and Safety Records

Item 06-714: Employee Assistance Program (EAP) counseling records. Records related to employee performance or conduct. Records of individuals who have sought or been referred to counseling services provided through the Employee Assistance Program (EAP). May include records of family members and dependents. Records of counseling services provided through the EAP for performance or conduct reasons. Records include documentation of: leave and attendance, performance,
alleged inappropriate behavior or workplace violence, reason for referral, management interventions, illegal drug or alcohol use, test results for use of illegal drugs, test results for alcohol consumption on the job, substance abuse assessment, treatment, aftercare, and monitoring records.

Disposition: Destroy once employee has met condition(s) specified by agreement or adverse action or performance-based action case file has been initiated.

Disposition Authority Agency (DAA): DAA-GRS-2017-0010-0014

Item 06-715: Employee Assistance Program (EAP) counseling records. Records not related to performance or conduct.
ho have sought or been referred to counseling services provided through the Employee Assistance Program (EAP). May include records of family members and dependents.
Records documenting nature of an individual's problem and participation in a treatment or rehabilitation program. Records may include documentation of treatment by a private therapist or a therapist at a Federal, State, local government, or private institution. Includes: Privacy Act and signed written consent forms, psychosocial history and assessments, medical records, correspondence with the client, clinical and education interventions, records of attendance at treatment, kinds of treatment, and counseling programs, identity and contact information of treatment providers, name, address, and phone number of treatment facilities, notes and documentation of internal EAP counselors, insurance data, intervention outcomes
Disposition: Destroy 7 years after termination of counseling for adults or 3 years after a minor reaches the age of majority, or when the state-specific statute of limitations has expired for contract providers subject to state requirements, but longer retention is authorized if needed for business use.

Disposition Authority: DAA-GRS-2017-0010-0015

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

Physical Controls: The information technology (IT) hardware used to host EAP CMS information is located in a secured data center facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software provisioned for EAP CMS is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access