US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/10/2025

OPDIV:

NIH

Name:

Enterprise Resource Planning System

PIA Unique Identifier:

P-9920482-362490

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.

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

Significant System Management Change

Describe in further detail any changes to the system that have occurred since the last PIA.

The Cost Point application was removed from the system boundary propelling the removal of information types related to Financial data, Human Resource and Payroll data.

Describe the purpose of the system.

The Enterprise Resources Planning System (ERP) is a collection of capabilities and applications that are responsible for collecting, storing, managing business activities for the National Cancer Institute at Frederick (NCIF). ERP consists of the following capabilities and applications: CognosBI (Business Intelligence), Cognos TM1, PSRS (Purchase Support Request System), FFS (Frederick Funding Solution) and Maximo.

ERP is used to access the following types of information about workforce contracts and direct contractor information: Budget, financial analytics, work order management, project/task

management.

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

ERP is a NCIF-wide data warehouse that contains direct contractor personnel, workflow, budget, and Equal Employment Opportunity (EEO) Information.

The ERP data warehouse contains the following Personally Identifiable Information (PII) about employees (direct contractors): names, birth dates, addresses (mailing & email), phones, employment status, certificates. This information is received from a downstream only flow of data from the source system, Cost Point. Cost Point used to be part of the ERP but not longer is. It is run as a separate entity providing minimum PII to ERP to create aggregated reporting. Cost Point maintains its own privacy impact assessment (PIA).

Information is used to conduct the following internal activities:
Reporting - generating reports for each of the types of the data ERP contains.
(Analyzing - the data contained in the reports can be used by managers to analyze subjects such as retirement trends and employee counts.
External organization information requests - required recurring reports and ad hoc requests for authorized external organizations.

ERP uses specific login information to assign permissions/user roles which is considered PII. However, this is done by using NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in an encrypted format. The IAM is 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 Enterprise Resources Planning System (ERP) is a collection of capabilities and applications that are responsible for collecting, storing, managing business activities for the National Cancer Institute at Frederick (NCIF). ERP consists of the following capabilities and applications: CognosBI (Business Intelligence), Cognos TM1, PSRS (Purchase Support Request System), FFS (Frederick Funding Solution) and Maximo.

ERP is used to access the following types of information about workforce contracts and direct contractor information: Budget, financial analytics, work order management, project/task management.

ERP is a NCIF-wide data warehouse that contains direct contractor personnel, workflow, budget, and Equal Employment Opportunity (EEO) Information.

The ERP data warehouse contains the following Personally Identifiable Information (PII) about employees (direct contractors): names, birth dates, addresses (mailing & email), phones, employment status, certificates. This information is received from a downstream only flow of data from the source system, Cost Point. Cost Point used to be part of the ERP but not longer is. It is run as a separate entity providing minimum PII to ERP to create aggregated reporting. Cost Point maintains its own privacy impact assessment (PIA).

Information is used to conduct the following internal activities:
Reporting - generating reports for each of the types of the data ERP contains.

(Analyzing - the data contained in the reports can be used by managers to analyze subjects such as retirement trends and employee counts.
External organization information requests - required recurring reports and ad hoc requests for authorized external organizations.

ERP uses specific login information to assign permissions/user roles which is considered PII. However, this is done by using NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in an encrypted format. The IAM is 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
Certificates
Employment Status

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose of PII collection is used to create reports so that users can analyze business and employee (direct contractor) trends.

These reports are primarily aggregated and de-identified. Using the PII to create visual representation of trends.

Some reports do have PII. Those reports are only created and released to users that are authorized to see the data.

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

NA

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

5 U.S.C. 301. ;42 U.S.C. § 3502 c; 31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301; Pub. L. 100–202, Pub. L. 100–440, and Pub. L. 101–509

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.

09-90-0024 Financial Transactions of HHS Accounting and Finance Offices

OPM/GOVT-1, General Personnel Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

NA

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.

ERP is not the source system. Cost Point is. Cost Point maintains the process for notifying individuals that their PII is collected.

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 is no option for individuals to opt out of the collection of PII since ERP is not the source system for collection. Cost Point is the source system and maintains their own opt-out processs. However for the use of their PII ,some secondary PII fields like Phone number and email address are optional and entered as a convenience.

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 because ERP is not the source system. Cost Point is the source system and maintains processes to obtain consent when a major change occurs.

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 concerns, they can reach out to the ERP system owner. However, ERP is not source system. Cost Point, as the source system, will maintain processes to resolve concerns.

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

Employees (direct contractors) will be able review and update personal information anytime through the Employee Self Service (ESS) Portal.

Cost Point, as the source system, will maintain a process for preiodic reviews of PII.

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 limited by job role with approval by system owner or designated representative. Temporary access granted to troubleshoot specific issue such as a data integrity concerns.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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 awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

All users are required to take role-based training and are required to follow documented processes.

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.

ERP maintains records in accordance with Records Retention Schedule 06-201, Employee Management Administrative Records that specifies to destroy within 3 years but can be kept longer if authorized for business use. Disposition Authority: DAA-GRS-2017-0007-0001.

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

Starting with the administrative controls, access to PII is limited by only allowing authorized users into the system. The ability to view or change specific PII fields is restricted to designated roles, such as the Payroll team can change employee bank account information while the HR team cannot. There is a process in place to remove access when employee transfers or terminates. Access is limited by job role with approval by the system owner or designated representative. Upon approval, access is provisioned only by ERP System Administrators.

The NIH Security Awareness Training course is used to satisfy the data privacy training requirement. According to NIH policy, all personnel who use NIH applications must complete security awareness training as part of the employee on-boarding process and then take an refresher training annually. This training includes sections on Information Security, Privacy Awareness, Counterintelligence, and Records Management.

Data Minimization Controls in place for the ERP are designed to reduce the potential exposure of PII. This limits the collection and retention of PII to the minimum elements needed to perform the operational function. One specific process in place cleanses PII data from ERP test environments.

For Technical Controls, Multi-factor Authentication requires the use of a physical card (PIV) along with a PIN to logon to the users workstation and the NCIF network required for access to the ERP. The ERP servers have Network Firewalls in place that limit the accessibility to other internal network computers. These Firewalls also require any transmission of PII to be encrypted. The Oracle Database that houses all ERP PII is encrypted as well in order to protect the data at rest. Lastly, detail logs of system and user activity are created in order to audit access and usage of PII throughout the ERP system.

And finally relating to Physical Controls, the data centers that house the ERP systems are protected by armed guards, fences, and other physical barriers. The data centers themselves require key cards for entry. Entry and exit by personnel is logged as part of the building access system.