US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/18/2024

OPDIV:

NIH

Name:

CIT Billing System

PIA Unique Identifier:

P-3998520-443513

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?

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 Center for Information Technology (CIT) Billing System (CIT Billing) allows for the recording, storage, classification, retrieval, creation, and transfer of fee-for-service billing records relating to the CIT Service Areas to the NIH Business System (NBS) for payment processing. NBS is the accounting source system for NIH.

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

The CIT Billing system collects, maintains, and shares:

Institute, Center and/or Office (ICO)/Agency code
CIT account number

Name
Office Address
NIH E-mail Address
Phone number
NIH Badge identification (ID) Number
NIH User Name
Hosting charges
Fee-for-Service transaction data
Service billing transaction data
Monthly and customized billing reports
Billing Records

CIT Billing staff upload a billing file to the NBS which in turn, bills and collects payments from the ICOs. Billing records contain CIT Account information for aggregating billing charges and exporting to NBS system. NBS is the source accounting system and maintains its own unique privacy impact assessment (PIA) on file with all legal authorities documented.

Those requiring access log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, with 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.

CIT Billing allows for the recording, storage, classification, retrieval, creation, and transfer of fee-for-service billing records relating to the CIT Service Areas to the NBS for payment processing. NBS is the accounting source system for NIH.

The CIT Billing system collects, maintains, and shares:
ICO/Agency code
CIT account number
Name
Office Address
NIH E-mail Address
Phone number
NIH Badge ID Number
NIH User Name
Hosting charges
Fee-for-Service transaction data
Service billing transaction data
Monthly and customized billing reports
Billing Records

CIT Billing staff upload a billing file to the NBS which in turn, bills and collects payments from the ICOs. Billing records contain CIT Account information for aggregating billing charges and exporting to NBS system. NBS maintains its own unique PIA on file with all legal authorities documented.

Those requiring access log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Mailing Address
Phone Numbers
NIH User Name, NIH Badge ID Number
ICO/Agency code, CIT account number, Hosting charges, Fee-for-Service transaction data
Service billing transaction data, Monthly and customized billing reports, Billing Records

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?

100-499

For what primary purpose is the PII used?

Personally identifiable information (PII) is used for billing contact, processes such as aggregating billing charges, and exporting to the NBS system.

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

There are no secondary uses for the PII.

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

Sections 301 and 302 of United States Code (U.S.C.), Title 5, Sections 3101and 3102 of United States Code (U.S.C.), title 44, and Executive Order 9397 (Nov. 22, 1943) authorize the Secretary to implement and establish the use of accounting systems at NIH.

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.

09-25-0217 NIH Business System (NBS)

Identify the sources of PII in the system.

Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

Sections 301 and 302 of United States Code (U.S.C.), Title 5, Sections 3101and 3102 of United States Code (U.S.C.), title 44, and Executive Order 9397 (Nov. 22, 1943)

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Not applicable. Systems are internal to NIH.

Describe the procedures for accounting for disclosures.

Not applicable. Data is not shared outside the agency.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Users submit their name and email address to NBS for access to system. This process is covered under the unique privacy impact assessment for NBS.

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 method in place. Individuals cannot access system if they opt-out of the collection or use of their PII.

Business entities cannot be enrolled in the CIT Billing system if they don't provide the necessary information.

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

No major changes have occurred to the system. Should there be a need for user notifications, they will be notified via email.

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 users believe that their names and email addresses have been inappropriately obtained, they can submit a ticket to the NIH IT Service Desk to have their account removed from the application. Or, they may contact the NIH Privacy Office 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.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. NIH username is for tracing who make changes to data.

The application support team periodically reviews the list of authorized users to confirm that they are still active users. If they are no longer active, their account is removed.

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.

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.

Application administrators and billing staff have access to all PII information in the application.

Customer/Read Only users only have access to their own PII information.

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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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 can receive additional training from key users within their business units.

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 Schedule.

Item 05-101: Financial Management and Reporting Administrative Records.
Records related to managing financial activities and reporting. Records include correspondence, subject files, feeder reports, workload management and assignment records.
Disposition: Destroy when 3 years old, but longer retention is authorized if needed for business use.
DAA-GRS- 2016-0013- 0001.

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

Physical controls include 24x7 guards of mobile units used to collect data, Personal Identify

Verification (PIV), key cards and closed circuit television (TV).

Technical controls include User ID, passwords, network firewall, Virtual Private Network (VPN), Intrusion Detection System, Role Based Access Controls, System logs.

Administrative controls include system security and contingency plan. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices, least privilege through role-based access, and policies for retention and destruction of PII.