US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

CMS

Name:

Incurred But Not Reported Survey System - Medicaid

PIA Unique Identifier:

P-4813973-155478

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?

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?

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.

Not applicable.

Describe the purpose of the system.

The Incurred But Not Reported Survey (IBNRS) system is a web-based application used by CMS to report estimated expenditures annually for the Medicaid Program and Children's Health Insurance Program (CHIP). The IBNRS collects and stores information on estimated annual Medicaid expenditures incurred by the states, but not yet paid by CMS at the end of the fiscal year. CMS uses IBNRS to prepare its fiscal year Annual Financial Report as required by Public Law 103-356, (the Government Management Reform Act of 1994 Section 3515).

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

The IBNRS system contain two categories of information: user credentials and the reported financial information from state Medicaid and CHIP programs.

The user credential information collected and stored in the application is: name, email address, user ID and password.

The financial information collected and stored within IBNRS is Medicaid and CHIP accounts payable and accounts receivable data from each state. The states submit two forms that contain the payment information: CMS-R199 Medicaid Accounts Payable and Accounts Receivable Form and CMS-10180 CHIP Accounts Payable and Accounts Receivable Form. The data includes information about drug rebates, overpayment amounts to providers, approved payments for Medicaid services, outstanding payments and other payment types. The information is in an 'aggregated' state and doesn't identify anything other than monetary amounts.

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

CMS uses IBNRS to prepare its fiscal year Annual Financial Report as required by Public Law 103-356. IBNRS collects, reports, and exports information on estimated annual Medicaid expenditures incurred by the states, but not yet paid by CMS at the end of the fiscal year.

The information collected and stored within IBNRS is Medicaid and CHIP accounts payable and accounts receivable data from each state. The states submit two forms that contain the payment information: CMS-R199 Medicaid Accounts Payable and Accounts Receivable Form and CMS-10180 CHIP Accounts Payable and Accounts Receivable Form.

IBNRS users, CMS employees, direct contractors and authorized state employees, access the system with user credentials. State users are given a [.]gov user ID. User credentials are stored and maintained for the length of time the user is authorized to utilize and access IBNRS.

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

User ID and password

CMS User ID

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?

The primary purpose of the PII is for a IBNRS system user to create an account and to access that account.

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 Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Business email not subject to Privacy Act

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

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB 0938-0988 expiration date 4/30/2017

OMB 0938-0697 expiration date 6/30/2016. This form is currently in the re-approval process and we have been advised that it is still considered 'approved' until a final date is populated in reginfo.gov This is the 9th renewal of the form.

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.

There is no direct process in IBNRS to notify individuals that their personal information is being collected. However, to obtain access to the system, the individual completed the CMS Form of Acceptable User Policy and was granted a CMS Enterprise User Administration (EUA) user ID and password. During that process of gaining access to CMS systems, individuals are notified that personal information 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.

Because an individual's PII (user ID and password) is required for access to and use of IBNRS, there is no 'opt out' method.

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

If there was a major change to IBNRS that affected the use and/or disclosure of system users' PII, the individuals would be notified by normal CMS methods: user-wide email alerts and notification within the IBNRS system welcome page. However, obtaining 'consent' isn't part of the process, because PII is required to access CMS systems.

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 about their PII they may contact the designated Point of Contact (POC) shown on the IBNRS final Welcome page and describe the concern. They may also contact the CMS IT help desk, by telephone or email and describe the concerns. The help desk and/or POC would investigate the concern and determine if any further steps were needed.

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

In order to maintain the accuracy, and relevancy of the PII stored within the database, a system administrator, performs a comparison of approved users with the EUA listing of individuals with IBNRS access every 180 days. Any anomalies (i.e. name change, or mismatch) are addressed and resolved by contacting the user, and either the user or the administrator updates the PII, or by removing their access to IBNRS, if no longer required under their current job description. Additionally, the data integrity and availability is maintained by employing security technologies including firewalls, and encryption and system access logs

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

Administrators:

System administrators have limited access to PII to manage user accounts.

Contractors:

Direct contractors, in their role as an administrator, would have limited access to PII to manage user accounts.

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

IBNRS uses role-based access permissions to determine which system users may access PII. It is solely limited to CMS employees and/or direct contractors in the role of system administrator.

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.

User account permissions limit the display of PII to only those elements needed to perform specific tasks. Also, IBNRS implements role-based access controls and auditing to ensure those with access have a "need-to-know" and a "need to 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.

All IBNRS users are required to complete the annual CMS Security and Privacy Awareness training provided annually as Computer Based Training (CBT) course. Contractors also complete their annual corporate security training.

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

Not applicable.

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.

Record retention for IBNRS follows the National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.2 item 30, which states that records will be destroyed or deleted Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate for system access records and the IBNRS data report files are pending NARA disposition authority.

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

The administrative controls in place to secure the PII include role-based access control, periodic review of users and deletion of non- active accounts, and rules of least privilege.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users to log into the application and a tiered system architecture which means users can only log into the application but not into any test environment and the testing and active applications are not joined together.

The physical controls in place are as follows: the IBNRS is hosted in a CMS secure data center. The data center has exterior security controls- video monitoring, the use of security cards, pass codes, and security guards

Note: web address is a hyperlink.