US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/02/2016

OPDIV:

CMS

Name:

Medicaid and Children's Health Insurance Program Budget and Expenditure System

PIA Unique Identifier:

P-4545735-648690

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 Medicaid and Children’s Health Insurance Program Budget and Expenditure System (MBES/CBES) is a web-based application that Medicaid state agencies use to report budgeted and actual expenditures for Medicaid and the Children’s Health Insurance Program (CHIP) to CMS, as required for the implementation of the Medicaid portion of the CHIP Program and Title XIX and XXI of the Social Security Act.

MBES/CBES uses the information from each state to compute the amount of Federal Financial Participation (FFP) CMS will provide to the state to fund program operations. The MBES also stores the state’s historical budget and expenditure records for data analysis purposes.

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

The information that MBES/CBES collects and stores is state Medicaid program financial information. The financial information is uploaded directly into the MBES/CBES system by a designated state user. There are four forms that are uploaded and are described below. The information contained within MBES/CBES is not broken down to the recipient or provider-detail level and does not contain any information that can identify any individual.

MBES/CBES is made up of the following forms that the states submit quarterly to CMS:

CMS-37 - Medicaid Program Budget Report Form CMS-37 is a financial report updated quarterly. It provides an estimate for both the current fiscal year and the budget fiscal year. After reviewing a state's submissions, CMS provides the state with a grant award that authorizes Federal funding for that particular quarter.

CMS-64 - Quarterly Medicaid Statement of Expenditures for the Medical Assistance Program is an accounting statement that contains the following information: the amount of Medicaid grant funds that have been dispersed for a given quarter, as well as past fiscal years; the recovery of funds or refunds provided; and the income earned on grant funds.

CMS-21 - Quarterly Children's Health Insurance Program Statement of Expenditures for Title XXI Form CMS-21 is an accounting statement that shows a state's recorded expenditures and disposition of Federal funds. Most of the expenditures reported on this form are associated with starting and expanding health insurance coverage to include uninsured, low- income children through the CHIP. States are entitled to Federal reimbursement based on the actual expenditures shown in this form.

CMS-21B - CHIP Program Budget Report Form CMS-21B provides states with a means to report on their program budgets and is used to estimate program expenses. Reconciliations between the projected program expenses shown in CMS-21B and the actual program expenses shown in CMS-21 are made after the period of availability for allotments has expired.

MBES/CBES also collects User IDs and passwords from users to access the system.

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

The MBES/CBES is an online system which allows the Medicaid state agencies to report budgeted and actual expenditures for Medicaid and the Children's Health Insurance Program (CHIP) to CMS, as required for the implementation of the Medicaid portion of the CHIP and Title XIX and XXI of the Social Security Act.

MBES/CBES uses the information from each state to compute the amount of Federal Financial Participation (FFP) CMS will provide to the state to fund program operations. The MBES also stores the state's historical budget and expenditure records for data analysis purposes.

MBES/CBES stores Medicaid budget and expenditure information that is summarized across the various categories of service. The information contained within MBES/CBES is not broken down to the recipient or provider-detail level and is not considered personally identifiable information (PII). Designated state personnel upload information into MBES/CBES through the forms described below. CMS reviews and certifies the information.

CMS-37 - Medicaid Program Budget Report. Form CMS-37 is a financial report updated quarterly. It provides an estimate for both the current fiscal year and the budget fiscal year.

CMS-64 - Quarterly Medicaid Statement of Expenditures for the Medical Assistance Program. It is an accounting statement that contains information about grant funding.

CMS-21 - Quarterly Children's Health Insurance Program Statement of Expenditures for Title XXI. This form is an accounting statement that shows a state’s recorded expenditures and disposition of Federal funds. States are entitled to Federal reimbursement based on the actual expenditures shown in this form.

CMS-21B - CHIP Program Budget Report. It provides states with a means to report on their program budgets and is used to estimate program expenses.

System users are CMS employees, CMS direct contractors and specifically authorized Medicaid state agency personnel. Each user has a User ID and password 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.

Name

E-Mail Address

Other - Job Title, User ID, Password

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 PII is required to create a user account within MBES/CBES, which allows the user to access the application.

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 Section 301, Departmental Regulations

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

No

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 0938-1265, expires 12/31/2017. It applies to the four CMS forms used to upload information into MBES/CBES: CMS-37, CMS- 64, CMS-21 and CMS-21B.

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.

Individuals are notified that their personal information will be collected, when they request permission through CMS to have access to MBES/CBES. There is also a warning banner at the log on screen that warns the user that they are accessing a government system.

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 to opt-out of the collection of PII because the individual's User ID and password are required to access MBES/CBES.

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

If a major change to MBES/CBES system were to occur that affected the users' PII, an email notification would be sent out as an alert message.

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.

After the initial log on screen, there is a welcome screen which provides MBES/CBES Point of Contact (POC) information. If an individual has concerns, they are instructed to contact a POC. Additionally, an individual would contact the CMS IT help desk by telephone or email to report any concerns. The help desk would investigate and determine if additional action is needed or whether it was resolvable by the individual updating their account 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.

To ensure the accuracy and relevancy of the PII, all MBES/CBES user accounts (PII) are reviewed every 180 days and compared to the CMS Enterprise User Administration (EUA) system permissions. Additionally, to ensure the availability, the list of active users is reviewed every 60 days. Integrity is ensured through the use of encryption, role-based access and restricting access to a limited set of authorized users.

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

Administrators:

System administrators have access to PII to communicate with the users via email and to manage access.

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

Access to PII is restricted based on role-based permissions. Only the system administrators have access to PII for communication with the users or for system operation and/ or maintenance.

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.

The system employs the concept of 'least privilege' so that only those administrators tasked with user maintenance can access the minimum amount of information necessary to perform their job. No others can access the PII.

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.

CMS employees and direct contractors are required to take annual Security and Privacy Awareness training. There is an exam at the conclusion, so that completion can be verified. In addition to that, there is a MBES/CBES User Guide for all registered users to read and review

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.

MBES/CBES are pending, per the CMS Records Schedule, published in April 2015. As such, MBES/CBES follows the National Archives and Records Administration (NARA), General Records Schedules (GRS) 3.1, 3.2, 4.1 and 4.3 which state that records will be destroyed or deleted as soon as "when no longer needed" or up to as long as 20 years 6 months old or when no longer needed for business, whichever is later

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

The MBES system is part of a virtual data center (VDC), which is a secured facility. Physical controls are in place such as security guards, the use of identification badges for entry, video surveillance and climate control measures.

The technical controls in place include intrusion detection and prevention technology (IDS/IPS), encryption, monitoring and system logs of activity, and virus/malicious code detection software.

Administrative controls are role-based access, training, periodic review of user accounts and written policies and procedures.