US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/19/2016

OPDIV:

CMS

Name:

Local Coverage Back End Database

PIA Unique Identifier:

P-7723786-700459

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?

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 Local Coverage Back End (LCBE) Database is the sole method for developing, collecting and finalizing local coverage policies used by the Medicare Administrative Contractors (MAC) to adjudicate and pay claims. The LCBE serves as a workspace, repository and policy record for the agency's local coverage policies.

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

The LCBE contains policy information on a wide variety of clinical topics across the Part A, Part B and Durable medical Equipment (DME) MACs. Information includes dates policies were opened in draft, responses to comments on policy, effective and revision dates, covered and non-covered diagnosis and procedure codes and related information to maintenance of the effective policies. LCBE uses login email addresses and passwords for LCBE users (Medicare Advantage Contractors (MAC) staff, Fu Associates, Ltd. (contracting company) staff, and limited CMS personnel).

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

The production LCBE is a major CMS owned FISMA application hosted by Amazon Web Services (AWS) at their public cloud facility located at Herndon, Virginia. The site is provisioned within a Virtual Private Cloud that in turn resides within the larger AWS owned Federal Risk and Authorization Management Program (FedRAMP) compliant hosting environment, which has been granted a cloud hosting Authority To Operate (ATO) by DHHS. The system retains all Local Coverage Database (LCD) policy and article versions created and saved by Medicare Administrative Contractors (MAC). The system does not allow a policy that has displayed on the CMS Medicare Coverage Database (MCD) to be deleted; all approved document versions remain on the LCBE permanently. MAC contractors may access their policy information as long as they hold the MAC jurisdiction contract. Contractors have access to the LCBE on a 24 by 7 basis using a login email and password. The system only allows sharing amongst LCBE users within a predefined set of parameters which are approved by CMS Center for Clinical Standards and Quality (CCSQ).

Access to the LCBE Database is limited to MAC staff, Fu Associates, Ltd. (contracting company) staff, and limited CMS personnel upon approval by CMS CCSQ. Approved document versions flow to the CMS Medicare Coverage Database (MCD) on a pre-defined weekly schedule for the general public to view.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

E-Mail Address

Other - passwords

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The LCBE user logon e-mail addresses and passwords contained in the LCBE are used for user access and to send e-mail notifications to users, relaying information, facilitating identification and password resets.

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

None

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

42 CFR 405.1060; section 1869(f)(2)(B) of the Social Security Act

5 U.S.C. 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

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A. There is only one PII data element (email), and therefore the collection is exempt from the Federal Paperwork Reduction Act's (PRA) "rule of 9" requirement.

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.

The Medicare Administrative Contractor (MAC) contract stipulates the use of the MCD. MAC employees agree to use the MCD as terms of their role and employment at the MAC. Similarly CMS employees that hold administrator roles for the system do so as part of their assigned duties.

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.

The only PII collected is credentialing information which is used for system identification and notification purposes. The credentialing information is necessary to perform job duties.

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

Individuals are notified by e-mail that the system is retaining their e-mail address or if a change in information has occurred. The system contains no other PII.

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 the e-mail address the user supplied is inaccurate, the user may inform a system administrator or the LCBE help desk. Since the information is already widely publicly available on other HHS and non-HHS websites (see URL examples above), there is no mechanism by which the information could be inappropriately obtained, used or disclosed from the secured LCBE.

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

MACs and system administrators are required to periodically review e-mail addresses for accuracy (every 6 months). Additionally, e-mail addresses are reviewed upon the departure or entry of a new MAC, Fu, or CMS employee that will be granted access to the LCBE. Passwords automatically expire every 60 days if the user account has not been used. User accounts are automatically disabled if the account is inactive for 90 days. Disabled accounts that have not been accessed in 365 days are manually removed from the database based on review by Administrative Users and Access Control Policies and Procedures.

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

Users:

The individual user may access only his/her own e-mail address to validate accuracy of e-mail address, and to validate user identity as CMS, Fu or MAC employee.

Administrators:

To administer security controls on LCBE system.

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

Only administrators may access the e-mail addresses of the users. Administrator access is the highest level permission in the system and is restricted to a select number of users with advanced training of security controls and compliant data management protocols.

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 only PII collected is credentialing information. Access to this information is controlled by permissions granted in the system.

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.

Annual CMS Security and Privacy Awareness training on internal controls and privacy awareness, security protocols, including table top testing of contingency plans related to potential breach for CMS employees, Fu staff, and MACs.

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

Users perform initial security training with refresher courses annually, and annual role based security training for personnel with assigned security roles and responsibilities.

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.

National Archives Records Association (NARA), General Records Schedule (GRS) DAA-GRS- 2013-0006-0003 states records will be destroyed 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.

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

The credentialing information retained in the system, which is the only PII collected by the LCBE, are secured by permission level access that is only granted to system administrators. LCBE conforms to a variety of security controls as required by FISMA and the CMS Security Program. Operational controls include but are not limited to: contingency plans and annual testing, backups of all files, offsite storage of backup files, physical security including secure buildings with access cards for entry, secure data center requiring additional access permissions for entry, security guards, background checks for all personnel, incident response procedures for timely response to security and privacy incidents, initial security training with refresher courses annually, and annual role based security training for personnel with assigned security roles and responsibilities.

Technical controls include but are not limited to user authentication with least privilege authorization, firewalls, Intrusion Detection and Prevention systems (IDS/IPS), hardware configured with the National Institute of Standards and Technology (NIST) security checklists, encrypted communications, hardware configured with a deny all/except approach, auditing, and correlation of audit logs from all systems. Management controls include but are not limited to: Assessment and Authorization (A&A), annual security assessments, monthly management of outstanding corrective action plans, ongoing risk assessments, and automated continuous monitoring.