US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/04/2016

OPDIV:

CMS

Name:

Durable Medical Equipment Prosthetics, Orthotics and Supplies Bidding System

PIA Unique Identifier:

P-1222392-611640

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?

Yes

Identify the operator.

Agency

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.

There have been no system changes since the last Privacy Impact Assessment (PIA).

Describe the purpose of the system.

Durable Medical Equipment Prosthetics, Orthotics & Supplies Bidding System (DBidS) is a web application for Durable Medical Equipment (DME) suppliers who wish to bid for specific product categories in a prescribed competitive bidding area. The bidding window is for a 60 day period, and those suppliers that do not participate or are not awarded a contract cannot bill Medicare.

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

The type of information the system collects includes the supplier’s organization and demographic information along with their bid data. Supplier’s organization and demographic data consists of the organization name, taxpayer ID, address, phone number(s), e-mail address and contact name(s).

Bid data consists of the type, quantity and price of certain durable medical equipment items.

In order to be granted access to the application, the user must provide their User ID and password. These 2 elements are maintained by a separate access control software and not the application. The separate access control software is called Enterprise Identity Management System (EIDM). The user also has a user role assigned to the dBids account.

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

The system collects supplier's organization and demographic information to determine which region of the country the supplier operates in.

Bid data is collected and evaluated based on the supplier's eligibility, its financial stability and the bid price. Contracts are then awarded to the suppliers who offer the best price and meet applicable quality and financial standards.

Users enter the application though a separate access control software that passes on the User ID, password and user role to the application. The User ID and user role is used to determine what type of access the user has to the application.

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

Taxpayer ID

Other: User ID, Password, and User Role.

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The User ID and Password allows the user to access the application. The User Role determines which data they can access.

The other PII information is used to contact the supplier(s) in order to notify them whether or not they won the bid for a contract with the government.

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.

Section 302 of the Medicare Modernization Act of 2003,
Medicare Improvements for Patients and Providers Act of 2008, The Affordable Care Act of 2010

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

No

SORN #09-70-0530, Medicare Supplier Information System

Identify the sources of PII in the system.

Online

Identify the OMB information collection approval number and expiration date

Office of Management and Budget #0938-1016; Expiration date: 11/2017

Is the PII shared with other organizations?

Yes

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

Private Sector

Provided to the Competitive Bidding Implementation Contractor (CBIC) who performs the bid evaluation for Competitive Bidding

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

All sharing or disclosures of system PII is governed by a signed Data Use Agreement between the government and the private contractor who evaluates all bids.

Describe the procedures for accounting for disclosures.

A record will not be created when PII is shared with another system or is disclosed outside the system because a signed Data User Agreement governs the use of PII data by the private contractors that maintains the application and evaluates the bids.

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

On the system login page, the user is presented with a Terms and Conditions page which notifies the individual that their personal information may be collected for lawful government purpose. This is presented prior to allowing the user to login to access the 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.

On the system login page, the user is presented with a Terms and Conditions page which notifies the individual that their personal information may be collected for lawful government purpose. There is an option to “Accept” or “Decline” the Terms and Conditions. Clicking on “Decline” will cancel the user’s login and they will not be allowed to access the system.

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

In the event the data uses have changed, notification will occur, and/or an opportunity for consent will be provided, before an individual’s PII will be used for a purpose materially different from that given at the time of collection. Notification will be provided in the form of an e-mail and/or letter to the user(s) impacted by the change at the time the change in use has been determined.

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 individual’s PII in the system has been inappropriately obtained, used, or disclosed; they may contact the Help Desk for assistance.

If the individual’s PII in the system is inaccurate, they may update the information they provided in the system up until the time of contract award. After the contract award is announced, they may contact the Help Desk for assistance in correcting their information by completing a Change of Information form.

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

Users of the system can review and/or modify their information anytime during the 60-day Bid Window. Before the close of the 60-day Bid Window, the user must certify that all information provided are true, accurate, and complete.

After the 60-day Bid Window, they are allowed to review, but not modify, their information for up to 90 days after bidding closes. This is to ensure the integrity of the data prior to having the bids evaluated.

Once the bids have been evaluated and the contract awards have been determined and announced, the data is kept for 90 days then removed/deleted from the system and no longer made available.

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

Developers:

To evaluate bid data.

Contractors:

To enter a bid and support Dbids

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

The system enforces role-based security.

The Help Desk role is granted by a government task lead (business owner) to the contractor responsible for assisting end users of the system.

The Developer role is granted by a government task lead (system owner) to the contractor responsible for maintaining the system.

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 enforces role-based security.

Contractors with the role of Help Desk have access to view user demographic and bid data in order to assist individuals with completing their bid.

Contractors with the role of Developer have access to view user demographic and bid data in order to support and troubleshoot any system issues.

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 Centers for Medicare & Medicaid Services personnel and contractors/business partners are required to receive general security, privacy awareness and Health Insurance Portability and Accountability Act (HIPAA) training. This includes, Annual HHS Information Systems Security Awareness Training, Annual HHS Privacy Training, Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgement; and Health Insurance Portability and Accountability Act training.

All training is provided and tracked online (computer based 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.

The Centers for Medicare & Medicaid Services General Support System adheres to data retention and destruction policies/procedures maintained by the Consolidated Information Technology Infrastructure Contract. Additionally, for the Provider/Supplier and Durable Medical Equipment Supplier Application

DISPOSITION:

a. Unprocessed applications as a result of provider/supplier failing to provide additional information - Destroy when 7 years old. (Disposition Authority: N1-440-01-1, Item 1a)

b. Approved applications of provider/supplier - Destroy 15 years after the provider/supplier's enrollment has ended. (Disposition Authority: N1-440-01-1, Item 1b)

c. Denied applications of provider/supplier. Destroy 15 years after the date of denial. (Disposition Authority: N1-440-01-1, Item 1c)

d. Approved application of provider/supplier, but subsequently, the billing number has been revoked - Destroy 15 years after the billing number is revoked. (Disposition Authority: N1-440-01-1, Item 1d)

e. Voluntary deactivation of billing number - Destroy 15 years after deactivation. (Disposition Authority: N1-440-01-1, Item 1e)

f. Provider/Supplier dies - Destroy 7 years after date of death. (Disposition Authority: N1-440-01-1, Item 1f)

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

Administrative control: The system enforces role based security. All Help Desk and Developer roles are reviewed weekly by a government task lead for appropriate access. Roles are removed from those contractors who no longer require it.

Technical control: All components of the application run in the Centers for Medicare & Medicaid Services Baltimore Data Center. The Data Center follows all cyber security protocols to protect agency data. Technical controls are in place such as the Data Center manages remote access, equipment ordering/testing, and has responsibility for the EUA system (management of user accounts), which defines the privileges for each user of the information system(s); OCISO coordinates compliance with security controls and the artifacts that document compliance by each application; and GSS manages, among others, telecommunications, remote access, and transmission confidentiality.

Physical control: Physical access to Centers for Medicare & Medicaid Services Baltimore data center are controlled by security personnel, electronic access cards and monitored via Closed Circuit TV.

Identify the publicly-available URL:

http://dbids.cms.hhs.gov/ (Note: The URL is only available during active Durable Medical Equipment Prosthetics, Orthotics and Supplies Bidding System bidding window).

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Web Beacons that do not collect PII.

Web Bugs that do not collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No