US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2026

OPDIV:

CMS

Name:

DMEPOS Competitive Bidding Program Systems

PIA Unique Identifier:

P-7264631-431460

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Initiation

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.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Competitive Bidding Implementation Contractor (CBIC) applications are central to the administration of the Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) Competitive Bidding Program (CBP). These applications are designed to support the Centers for Medicare & Medicaid Services (CMS) in managing the competitive bidding process for durable medical equipment, prosthetics, orthotics, and supplies.These applications support HHS program administration by managing the competitive bidding process for medical equipment and supplies used by Medicare beneficiaries. They enable CMS to collect and evaluate supplier bids, ensure that suppliers meet program requirements, and award contracts to qualified vendors.The system also supports oversight and compliance functions by tracking supplier performance, maintaining records of contracts and pricing, and helping ensure that services and equipment provided to beneficiaries meet established standards. In addition, the applications support communication and operations by facilitating coordination between CMS, contractors, and suppliers, and by providing tools to manage program activities efficiently.

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

CBES (Competitive Bid Evaluation System) houses bid data from Connexion and is used to objectively evaluate bid submissions. CMRS (Contract Management and Reporting System) imports results from CBES to support contracting tasks related to maintaining contracts during the contract performance period. The CBIC Admin Repository of Jobs is used across multiple internal CBIC applications and moves data used by these applications into the corresponding databases. The systems collect and maintain SSN, Name, Date of Birth (DOB), and Email Address, User ID, Role Information, and Organization Affiliation. Social Security Number (SSN), full name, date of birth (DOB), and email address. This information is used to identify and validate individuals participating in the competitive bidding process and to support program administration. User ID (username), role information, and organization affiliation. CMS Identity Management (IDM) User IDs are typically created at registration by the individual user and CMS Enterprise User Administration (EUA) IDs are generated by CMS EUA. Passwords are created and managed by the individual user in accordance with CMS security requirements. Role information and organization are assigned by system administrators at CMS and role requests within IDM to control access and permissions within the system. Information in the system is retained in accordance with CMS records retention policies and federal records schedules. In general, data is maintained for the duration of the contract lifecycle and for a defined retention period afterward to support auditing, compliance, and reporting requirements. User account information is retained for as long as access is required and is removed or deactivated when no longer needed.

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

The DMEPOS Competitive Bidding Program (CBP) Systems (DCBPS) is a collection of systems that operate interdependently to support the Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) CBP, encompassing education, registration, bidding, bid evaluation, contracting, oversight, and maintenance. The DMEPOS CBP is divided into phases, with each application corresponding to a set of business processes. These applications are connected by bidder and data, but each serves a specific purpose or SOW task.Information is collected to support the administration, evaluation, and oversight of the DMEPOS CBP by Centers for Medicare & Medicaid Services (CMS). For suppliers, the system collects business and identifying information including name, SSN, DOB, email address, and organization affiliation to verify identity, confirm eligibility, evaluate bids, and support contract award decisions. For IDM and CMS (EUA) users, the system collects user ID, role information, email address, and organization affiliation to manage access and enforce role-based permissions.The system also collects bid data, evaluation results, contract records, and reporting data to support objective bid evaluation (CBES), contract management and reporting (CMRS), and data processing (DCBPS Admin Repository of Jobs). Records may be retrieved using PII elements such as name, email, SSN, or user ID for evaluation, contract management, auditing, and support purposes. Access is restricted based on user roles. Connexion is the DMEPOS CBP's secure portal that suppliers use to submit bids and supporting documentation, while enabling CMS to manage bid reviews, evaluations, and contract award processes. CMS Division of DMEPOS Competitive Bidding (DDCB) users with a Connexion role can access information and documents. Connexion includes an eChat feature for secure communication between CSAs and Connexion users.Connexion Admin Repository of jobs used by Connexion.CBIC Bid Evaluation System (CBES) Houses bid data from Connexion and is used by CBIC reviewers to objectively evaluate bids and financial data, identify winners, disqualify bidders, and determine single payment amounts. CBES becomes a data repository after bidding is complete. This is an internal system with no public access.Contract Management and Reporting System (CMRS) Internal system used to import CBES results for contracting tasks and contract updates from Connexion. Used by CBIC associates and program managers throughout the contract performance period. No public access.Competitive Bidding Inquiry Tracking System (CBITS) CRM system for tracking telephone and written inquiries and complaints, primarily used by CSAs and CBIC Competitive Bidding Liaisons. Internal use only.Inquiry and Reporting Information System (IRIS) Data repository

containing identity information for querying registration data. Used by CBIC for reports and by CSAs to troubleshoot registration issues. Incorporated into CBITS for caller verification. IRIS houses all rounds of bidder registration data. Internal system with no public access.CBIC Admin Repository of jobs that moves data across multiple internal DMEPOS CBP applications to databases.CBIC Services Repository of web services used to access CBIC data across multiple DMEPOS CBP applications.

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

Yes

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

Social Security Number
Date of Birth
Name
E-Mail Address
Other: User ID – A unique identifier used to authenticate and authorize access., Role Information – Determines access level (e.g., Authorized Official (AO), Backup Authorized Official (BAO), End User (EU)), Organization Affiliation – Links the user to a supplier entity.

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?

PII is used to determine the supplier’s Identification, operating regionEvaluate eligibility, financial stability, and bid competitiveness.

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.

42 CFR 414.412 (CMS-1828-F)

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.

SORN 09-70-0530 - Medicare Supplier Identification File (MSIF)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Other
Government Sources
Other
Non-Governmental Sources
Other

Identify the OMB information collection approval number and expiration date

CMS-10169, OMB-0938-1016 Expiration date is July 31, 2028.

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

Describe the procedures for accounting for disclosures.

When users access Connexion, the system retrieves and associates' records based on the following PII elements provided by IDM.User ID – A unique identifier used to authenticate and authorize access.Full Name – Used to match user identity and roles.Email Address – For communication and account verification.Role Information – Determines access level (e.g., AO, BAO, EU).Organization Affiliation – Links the user to a supplier entity.Date of Birth and SSN – Required for registration and validation against the National Supplier Clearinghouse (NSC)Records are retrieved using PII during login, role validation, and bid management processes. HHS collects and maintains bidder information including SSN, in compliance with The Social Security Act and the Federal Acquisition Regulation (FAR) 4.603 & 52.204.

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

CMS Identity Management (IDM) collects and maintains bidder information. They manage user identities, authenticate access, and authorize activities within CMS systems, including bidding applications.

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.

Individuals will not be permitted to participate in the competitive bidding program. There is no opt out available for PECOS. Submission of PII is mandatory for bidding. PECOS operates under federal authority for the Centers for Medicare & Medicaid Services (CMS). The collection of PII is required to verify provider identity and qualifications, prevent fraud and abuse, and maintain accurate enrollment records for Medicare/Medicaid billing.

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

Suppliers will be notified by ListServ (Email) and can reference all information on www.dmecompetitivebid.com. In addition, CMS IDM remote identity proofing (RIDP) requests consent to verify identity information to complete the RIDP. Completing this allows the user to proceed with IDM registration.

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.

Suppliers can reach out to the CBIC Help Desk, via 877-577-5331 or cbic.admin@palmettogba.com if they believe their data has been inappropriately obtained, used, or disclosed, CMS will follow internal policy and complete the privacy and security incident form within 1 hour to begin an investigation. If the PII is inaccurate, we'd refer them to IDM via 1-888-734-6433 or NPEAST via 866-520-5193 or NPWEST via 866-238-9652 based on their assigned U.S. states and territories for assistance with supplier questions.

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

DCBPS Reports can be generated in the applications, to validate data quality, accuracy and any needed audit information. DCBPS has a structured process to bi-weekly review the collection,

use, storage, and protection of Personally Identifiable Information (PII) to ensure compliance with security, privacy, and regulatory requirements, by examining the applications and pulling reports for recordkeeping.

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.

The system implements a multi-layered access control procedure aligned with the DMEPOS Competitive Bidding Program requirements Role-Based Access Control (RBAC) Access to PII is determined through formal role assignment in CMS Enterprise Portal/IDM. Supplier users are assigned to one of three predefined roles Authorized Official (AO) Can enter data, approve bids, certify submissions, upload documents, and manage user access for their organization Backup Authorized Official (BAO) Same capabilities as AO, serves as backup End User (EU) Limited access - can enter data and upload documents but cannot approve or certify bids Each role has specific permissions defined in the Connexion User Role Table. Users can only access their own organization's PII based on their PTAN (Provider Transaction Access Number).Supplier Eligibility Validation Before granting system access, suppliers must Be Medicare-enrolled with valid CMS-855S enrollment application Have current enrollment information in PECOS (Provider Enrollment, Chain, and Ownership System)Designated Authorized Official must match PECOS records exactly (name, address, contact information)PTAN used for registration must be valid and active in PECOS. Registration Process Supplier access follows a formal registration procedure AO creates account in CMS Enterprise Portal with credentials. AO requests access to Connexion via portal. System validates PTAN and LBN against PECOS in real-time. Identity proofing through CMS RIDP (Remote Identity Proofing) questions. AO must approve all BAO and EU registration requests. Each user must use unique credentials (sharing prohibited).CBIC Staff Access Authorization Palmetto Government Benefits Administrators (GBA) CBIC staff access requires Supervisor approval documenting business need for specific role, Completion of CMS Security Awareness training, Background investigation appropriate to sensitivity level, Acknowledgment of Rules of Behavior, Annual recertification of access need, Access restricted by function (bid evaluators, contract specialists, customer service, system admins). Automated Access Reviews require quarterly automated reports identifying dormant supplier accounts and inactive CBIC staff access. Annual access recertification requires supervisors to validate that CBIC staff still require their current level of access. Supplier accounts are automatically disabled if PECOS enrollment lapses or becomes inactive. Technical Controls CMS Enterprise Portal authenticates all users with MFA and Connexion validate user roles and organization context database queries filter data by PTAN ensuring suppliers only see their own information CBIC staff access is logged with specific business justification codes.

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 dmecompetitivebid.com system implements the following minimum necessary controls Supplier Data Isolation Each supplier organization can only access their own PII based on their authenticated PTAN. Database-level row security filters ensure suppliers cannot query or view other suppliers' information. For example, when a supplier logs into Connexion to view their bid, the application

enforces PTAN-based filtering, so they retrieve only their own organization's bid forms (Form A and Form B), financial documents, and bid surety bonds - not other suppliers' bids. Role-Specific Function Access End Users (EU) Can enter bid data and upload documents but cannot view final bid amounts or certified submissions, cannot approve contracts, cannot access contract management functions post-award AO/BAO Can view full bid details for their organization, approve submissions, and manage contracts but cannot access other suppliers' data. CBIC Bid Evaluators Can access supplier PII only during active bid evaluation periods and only for suppliers who submitted bids in the current round CBIC Customer Service Can view limited supplier contact information and account status but cannot access financial documents or bid amounts Document Access Restrictions Financial documents and bid surety bonds uploaded to Connexion are encrypted at rest and access controlled. Only the uploading supplier organization and designated CBIC bid evaluation staff can view these documents. Documents are not accessible to customer service staff or system administrators unless explicitly authorized for a specific support ticket. Time-Based Access Limitations Supplier access to sensitive bidding functions is restricted based on program phase Pre-Bid Window Suppliers can register but cannot access bid forms Bid Window Open Suppliers can create and submit bids, upload documents Bid Window Closed Suppliers can view submitted bids (read-only) but cannot modify Post-Award Only contract suppliers can access contract management functions CBIC Staff Data Masking Customer service representatives see masked versions of sensitive supplier information (e.g., last 4 digits of tax ID numbers, masked bank account numbers from financial documents) when assisting with support inquiries. Full PII access requires supervisor approval and is logged. Audit Logging All PII access is logged to AWS CloudWatch Logs including User identity (CMS Enterprise Portal user ID)Organization (PTAN)Timestamp of access Specific data elements accessed (e.g., "viewed Form A financial information," "downloaded bid surety bond") Business justification code for CBIC staff access Progressive Disclosure in UI The Connexion interfaces display only PII fields necessary for current tasks. Full supplier profiles are not loaded on login instead; data is retrieved as users navigate to specific functions. For example, viewing the supplier directory shows only organization name and location - detailed contact information requires additional authorization.

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 dmecompetitivebid.com system users complete the Annual CMS Information Security and Privacy Awareness Training All CBIC staff (system owners, managers, operators, contractors) with access to the Connexion systems complete CMS's annual web-based training covering Privacy Act responsibilities for federal systems, Proper handling of Personally Identifiable Information (PII), HIPAA requirements (though DMEPOS supplier information is not PHI, training ensures understanding of broader CMS privacy requirements), Incident reporting procedures specific to CMS systemsPassword security and multi-factor authentication requirements, Social engineering awareness, and Secure handling of financial documents. CBIC Role-Based Training Upon Initial Access includes Bid Evaluators Receiving specialized training on confidentiality of supplier bid information, conflict of interest rules, proper handling of financial documents during evaluation, and secure destruction of evaluation materials.Contract Specialists complete training on contract supplier PII protection requirements, subcontractor disclosure handling, and privacy considerations in contract monitoring.Customer Service Staff complete training on providing assistance without accessing unnecessary PII, proper verification procedures before discussing account details, and escalation procedures for suspected fraud.System Administrators complete training on privileged access responsibilities, logging requirements, and emergency access procedures. Supplier User Training and Education While suppliers are not federal employees, CBIC provides comprehensive educational resources. Required acknowledgment of Terms and Conditions that include privacy responsibilities, Registration Reference Guide for Connexion explaining proper credential management, Webcasts and educational events covering secure document upload procedures, User guides emphasizing prohibition on sharing user IDs and passwords, and guidance on protecting bid

surety bond information and financial documents.Annual Refresher Training All CBIC staff complete annual recertification confirming understanding of PII handling requirements specific to supplier information, changes to competitive bidding program requirements that affect privacy,Updated threat landscape and social engineering tactics targeting competitive bidding programs, and Proper procedures for supplier identity verification before providing information.Training Documentation Training completion is tracked in CMS's learning management system. CBIC staff access to Connexion production systems is automatically suspended if annual training becomes overdue. Training certificates are maintained as evidence of compliance for ATO audits and CMS contract oversight reviews.

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

Beyond general security awareness training, dmecompetitivebid.com system users receive the following additional specialized training. CBIC Application-Specific Training (4 to 6 hours for new staff) This training covers Connexion architecture and data flows, PECOS integration and supplier validation, CMS Enterprise Portal and IDM authentication, proper use of bid evaluation tools, covered document review procedures, recognizing fraudulent bid submissions, and documenting supplier support interactions.Competitive Bidding Program Policy Training CBIC staff receive specialized training on Medicare DMEPOS Competitive Bidding Program requirements including 42 CFR Part 414 Subpart F regulations, supplier standards and enrollment requirements, confidentiality of bid information, fraud and waste and abuse indicators, and handling of bid surety bonds and associated financial information.AWS Cloud Security Training (Infrastructure and DevOps Staff) Technical staff complete AWS-specific training covering GovCloud and FedRAMP environment requirements, Secrets Manager for credential management, CloudWatch log monitoring, S3 bucket security for financial documents, and VPC network segmentation isolating production systems from the public website. PECOS Integration and Data Privacy Training Staff working with PECOS data complete training on data classification and handling, validating supplier information without retaining unnecessary PII, understanding PECOS enrollment data sensitivity, and incident reporting for data discrepancies.Bid Window Surge Training During active bid windows, customer service staff complete refresher training on handling increased call volume without compromising security, verifying supplier identity, guiding secure document uploads, and escalation procedures for last-minute technical issues.Financial Document Handling Training Staff with access to supplier financial documents complete training on handling sensitive business proprietary information, secure viewing procedures, recognizing personal financial information, secure destruction of printed materials, and preventing inadvertent disclosure.Training Frequency Core CBIC training is completed upon initial access and annually. Bid window refresher training occurs before each competitive bidding round. AWS security training is completed annually for technical staff. Program updates are provided quarterly when regulations change. Contractor-Specific Training Third-party contractors complete onboarding covering Palmetto GBA security policies, CMS contractor requirements, and non-disclosure agreements protecting supplier bid information.

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 Retention Schedules consist of supplier PII and competitive bidding data in the dmecompetitivebid.com system following CMS records retention requirements and National Archives and Records Administration (NARA) General Records Schedules. Active Bid Submissions are retained for 6 years after the bid window closes. Financial Documents uploaded to Connexion are retained for 6 years after bid evaluation completion to support audit trails and OIG investigations. Awarded Contract Supplier Records are retained for 10 years after contract expiration. Supplier Registration and Account Data are retained for 3 years after account inactivity. System Audit Logs are retained for 6 years per CMS security logging requirements. Bid Surety Bonds are retained for 6

years after return or forfeiture. CBIC Staff Access Records are retained for 3 years after account termination. Supplier Complaint Records are retained for 7 years after resolution.Destruction ProcessDatabase Records Automated processes identify records exceeding retention periods. Records flagged for deletion are moved to staging tables for a 90-day CMS review period. After CMS approval, DELETE operations permanently remove supplier records from production databases. Deletion actions are logged to maintain an audit trail without retaining actual PII content.Uploaded Documents Financial documents, bid surety bonds, and other files stored in encrypted S3 buckets are transitioned to S3 Glacier after bid evaluation. After the retention period expires, S3 objects are permanently deleted. S3 server access logs are deleted after 1 year.Backup Media AWS RDS Automated Snapshots are automatically deleted after the retention period. Manual snapshots are reviewed annually and deleted per retention schedules. Historical bid round data is retained in encrypted cold storage and destroyed after 10 years.Decommissioned System Components When systems are decommissioned, data sanitization follows NIST SP 800-88. ECS container storage is ephemeral and automatically destroyed on termination. RDS instances undergo secure deletion with a final encrypted snapshot sent to CMS. S3 buckets undergo versioning purge before deletion. Legacy System Data Migration Supplier PII required for new systems is securely migrated. Non-essential PII is destroyed per retention schedules before migration, and a data minimization review identifies PII no longer serving program purposes.CMS Records Officer Consultation For retention questions not clearly covered by existing NARA schedules, CBIC consults the CMS Records Officer at Records_Retention@cms.hhs.gov. CBIC provides a Certificate of Destruction to CMS documenting the records destroyed, retention schedule authority, destruction method, date, and authorizing personnel.

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

The dmecompetitivebid.com system secures supplier PII through comprehensive administrative, technical, and physical controls implementing NIST 800-53 Rev 5 for FISMA Moderate systems. Administrative Controls, The system operates under CMS Information Security Acceptable Risk Safeguards (ARS), Palmetto GBA security policies, and competitive bidding program-specific confidentiality requirements. Role-based access requires PECOS enrollment validation, CMS Enterprise Portal identity proofing, and annual recertification. CBIC staff complete annual mandatory training covering supplier PII protection, bid confidentiality, and financial document handling. Documented incident response procedures include a 1-hour CMS notification requirement and special procedures for bid information disclosure. A comprehensive System Security Plan documents all FISMA Moderate security controls. Quarterly security control assessments and monthly vulnerability scanning are conducted during bid windows.Technical Controls, CMS Enterprise Portal/IDM requires multi-factor authentication for all suppliers and CBIC users. TLS 1.2 /1.3 encrypts all web connections, and API connections to PECOS use mutual TLS authentication. RDS databases and S3 buckets are encrypted using AWS KMS and AES-256. Sensitive financial data uses column-level encryption with Oracle TDE, and all backups are automatically encrypted. Network segmentation uses a VPC with private subnets isolating the Connexion application tier from the public-facing website. Security Groups restrict database access to the application tier only. AWS WAF protects against OWASP Top 10 attacks with rate limiting and geoblocking. AWS GuardDuty monitors for malicious activity and unauthorized access attempts. Sessions time out after 30 minutes of inactivity and are invalidated on logout with server-side session destruction. PECOS integration uses OAuth2 service-to-service authentication. Responses are cached with encryption and expire after 24 hours. No permanent PECOS records are stored, and integration uses a dedicated VPN connection to the CMS network. Comprehensive CloudWatch logging captures all supplier PII access events. Logs are encrypted, tamper-resistant, and retained for 6 years. Vulnerability management includes SonarQube, Snyk, and AWS Inspector scans, with findings remediated per CMS severity timelines. AWS Secrets Manager handles automatic credential rotation with no hard-coded credentials in application code. Physical Controls, Connexion operates in AWS GovCloud or FedRAMP-authorized regions with SOC 2 Type II certified physical security, 24/7 surveillance, and

biometric server room access. CBIC offices include badge-controlled access, locked storage for printed supplier documents, secure shredding, and visitor escort requirements. Staff workstations use full disk encryption, automatic screen lock, and USB port controls. All backups are stored in geographically separated AWS regions with MFA-restricted access. Compliance Validation, Annual penetration testing, FISMA Moderate ATO with annual reassessment, continuous monitoring using CMS-approved tools, OIG audits, and GAO program effectiveness reviews verify privacy control compliance.