PTA / PIA: FDA - DMPBC - QTR2 - 2026 - FDA5271039

Created Date: 6/22/2026 6:13 PM Last Updated: 7/2/2026 6:00 PM

General Information

PTA / PIA Name:	FDA - DMPBC - QTR2 - 2026 - FDA5271039	**PTA / PIA ID:**	4586885
Component Name:	FDA - CTP OS Data Modernization Package Business Capabilities Platform	**ATO Boundary Name:**	CTP OS Data Modernization Packaged Business Capabilities Platform
Overall Status:	Complete	**# of Days - Open:**	29
Submitter:		**Submit Date:**	6/15/2026
Next Assessment Date:	07/01/2029	**Expiration Date:**	7/1/2029
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	8/20/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Yu Mei
PTA 01A:	POC Title and Organization	CTP/OS/DRSI System Owner
PTA 01B:	POC Email Address	Yu.Mei@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-5761
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	Significant System Management Change

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Since the last approved Privacy Threshold Analysis (PTA), Center for Tobacco Products (CTP) Office of Science (OS) Data Modernization Package Business Capabilities Platform (DMPBC) system has undergone several significant changes. The system now collects, maintains, and shares non-sensitive, external business Personally Identifiable Information (PII) (business emails, business Points of Contact (POC) names, business phone numbers and business addresses), whereas previously no PII was collected. The system has also integrated HALO, a central Databricks data warehouse supporting Food and Drug Administration (FDA)'s Intelligent Data Lifecycle Ecosystem (FiDLE) initiative. Additionally, the system now leverages artificial intelligence through the Office of Digital Transformation (ODT) Elsa Application Programming Interface (API) connection using Claude as the model. The system has also received an active Authorization to Operate (ATO) with a Federal Information Security Modernization Act (FISMA) moderate categorization since the last assessment.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Data Modernization Packaged Business Capabilities (DMPBC) platform aims to facilitate the development of data and application services in the form of packaged business capabilities (PBCs) designed to optimize access to enterprise data, as well as common Information Technology (IT) capabilities in the Office of Science (OS). DMPBC will increase agility and efficiency by making data and common IT capabilities available to OS, eliminating technical barriers and accelerating access to required data. In support of the Department of Health and Human Services (HHS), the DMPBC platform establishes a collection of OS Data Services used for tobacco review and regulation purposes, enabling the OS to expand and build IT applications quickly. The system provides common utilities such as authentication and authorization, which standardize and streamline the process of adding new data services to the platform. Additionally, the system extends the Operational Data Gateway Service (ODGS), a software solution that connects to multiple operational data sources and provides a single, central point of access. ODGS standardizes access to OS tobacco review data across different systems and is built with GraphQL technology, which provides the ability to fetch precisely the data the client needs. Finally, the DMPBC platform incorporates HALO, a central data repository built on Databricks that stores curated and trusted data for business intelligence purposes and agency-wide data sharing initiatives, including the Food and Drug Administration's (FDA's) Intelligent Data Lifecycle Ecosystem (FiDLE) services such as R-Studio (a software development environment), eMDM (an enterprise Master Data Management tool), and Trifacta (a data preparation and transformation tool). The DMPBC platform also leverages artificial intelligence (AI) through ODT's Elsa API connection, an internal FDA system using Claude as the underlying model. HALO serves as the underlying data source that feeds into the Elsa AI system, enabling Elsa to provide intelligent, conversational query capabilities that allow authorized FDA users to interact with and retrieve tobacco review and regulatory data in a more intuitive way, rather than requiring users to manually construct complex GraphQL or Representational State Transfer (REST) API queries. As ODT's Elsa is an internal FDA system operating within the same agency and Operating Division, it is not considered a third-party website or application (TPWA). The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The DMPBC system collects, maintains, and shares both non-personally identifiable information and non-sensitive Personally Identifiable Information (PII). With respect to non-PII, the system holds comprehensive descriptions and endpoint

definitions for all application packaged business capabilities, components deployed on the Office of Science's (OS's) Enterprise Architecture (EA) Service Platform Application Layer, and data hosted on OS's EA Service Platform Data Layer. Additionally, the system shares information stored in the Product Management System (PMS) and Rhapsody, which are operational data source systems. With respect to PII, the system currently collects and maintains non-sensitive external business PII on an ongoing basis, including business email addresses, business Points of Contact (POC) names, business phone numbers, and business mailing addresses. This business PII is sourced from the private sector and pertains to external regulated entities, such as industry vendors who submit Premarket Tobacco applications for product approval through FDA's Center for Tobacco Products (CTP) regulatory review process.

The system also leverages artificial intelligence (AI) through ODT's Elsa API connection, an internal FDA system using Claude as the underlying model. HALO serves as the underlying data source that feeds into the Elsa AI system, enabling Elsa to provide intelligent, conversational query capabilities that allow authorized FDA users to interact with and retrieve tobacco review and regulatory data. Further details on the AI tools and their use are provided in PTA-21A.

Users access the system using HHS/OpDiv Personal Identity Verification (PIV) cards, with user credentials maintained in Active Directory (AD) and access governed through Role-Based Access Control (RBAC) procedures. Internal FDA users access the system through the FDA intranet, as the system's URLs are not publicly facing. Direct Contractors within CTP and other FDA centers also have access to the system. All data is stored within the HALO central data warehouse, which is hosted in FDA Amazon Web Services (AWS) GovCloud. As HALO is a central data warehouse and not an original source of records, the retention guidelines for PII and non-PII stored within HALO are managed by the applicable source systems. For industry contact information (business email addresses, business POC names, business phone numbers, and business mailing addresses), data is retained for the duration of the associated regulatory matter plus seven years after the regulatory matter is closed or the product is removed from the market, whichever is later. For tobacco product submissions, records are retained for 30 years after cutoff in accordance with records schedule DAA-0088-2020-0001. Full retention schedules and destruction procedures are described in detail in PIA-44. All data is secured in accordance with Federal Information Security Modernization Act (FISMA) moderate controls under the Authorization to Operate (ATO) and System Security Plan (SSP) National Institute of Standards and Technology (NIST) controls.

PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The DMPBC platform provides a suite of data and application services designed to optimize access to enterprise data and provide essential capabilities for tobacco review and regulation. These data and application services serve as building blocks for large systems based on Composable Architecture, a framework to build, assemble, and reassemble business elements to meet user needs. The platform collects and maintains comprehensive descriptions and endpoint definitions for all application packaged business capabilities, components deployed on OS's EA Service Platform Application Layer, and data hosted on OS's EA Service Platform Data Layer.This information is collected to establish the DMPBC platform as a central repository of OS Data Services used for tobacco review and regulation purposes, enabling the OS to expand and build IT applications quickly. The system also provides common utilities such as authentication and authorization, which standardize and streamline the process of adding new data services to the platform. Information is shared with other systems through the Operational Data Gateway Service (ODGS), a software solution that connects to multiple operational data sources and provides a single, central point of access. ODGS standardizes access to OS tobacco review data across different systems and is built with GraphQL technology, which provides the ability to fetch precisely the data the client needs. Information is also shared with downstream systems including CTP Rhapsody, CTP Electronic Submissions (Esub), and the Center for Drug Evaluation and Research (CDER) Master Data Management (MDM) system, which require access to the data to process user application submissions. HALO serves as the central data warehouse under FDA's Intelligent Data Lifecycle Ecosystem (FiDLE) as the central location for cleansed data. With respect to PII, non-sensitive external business PII, including business email addresses, business POC names, business phone numbers, and business mailing addresses, is collected and maintained solely for the purpose of communicating with industry vendors who submit Premarket Tobacco or equivalent applications for product approval through FDA's CTP regulatory review process. This information is shared within HHS for the purpose of standardizing a global mailing address and a registration process for external vendor onboarding. No personal sensitive PII, such as Social Security Numbers (SSNs), is collected, used, processed, or transmitted by the

		system. Additionally, the current services provided do not require Division of Safety personnel who access or use the system to use any personal identifiers to retrieve records held in the system, nor are there plans for services that would require this. The system also leverages AI through ODT's Elsa API connection, an internal FDA system using Claude as the underlying model, to provide intelligent, conversational query capabilities that allow authorized FDA users to interact with and retrieve tobacco review and regulatory data in a more intuitive way. HALO's role as a repository of curated and trusted data provides the clean, structured data necessary to support reliable AI-driven responses. The collection and use of data in support of the Elsa AI connection does not introduce any new categories of PII beyond those already described above.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	The following URLs are associated with the CTP Data Modernization system. All URLs are internal and not public facing, accessible only via the FDA intranet with Single Sign-On (SSO) enabled. Production URLs: CTP API Directory UI: https://dmpbc.fda.gov/ctp-api-directory/ Operational Data Gateway Service (ODGS): https://dmpbc.fda.gov/odgs/actuator/health Appendix-A: https://dmpbc.fda.gov/appendixa-web-ui/signon Pre-Production URLs: CTP API Directory UI: https://dmpbc.preprod.fda.gov/ctp-api-directory/ ODGS: https://dmpbc.preprod.fda.gov/odgs/actuator/health Appendix-A: https://dmpbc.preprod.fda.gov/appendixa-web-ui/signon
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No

PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The CTP Data Modernization system includes several internal web-based applications, each serving a distinct purpose in support of tobacco review and regulation. The API Directory is a user interface application that lists all available Application Programming Interface (API) and Graph Query Language (GraphQL) queries that can be utilized to retrieve data from source systems such as the Product Management System (PMS) and Rhapsody, along with instructions on how to use them. Users are able to view available endpoints and query specifications but are not able to execute services directly from the user interface. The Operational Data Gateway Service (ODGS) includes the actual services and GraphQL queries that can be utilized for retrieving data from source systems. The Appendix-A application allows users to generate and download Appendix A reports, which are used by Regulatory Health Product Managers as part of communications to the industry and contain tobacco product lists that identify tobacco products within a submission. Access to all applications is restricted to internal FDA employees with a valid FDA email address. Direct Contractors within CTP and other FDA centers also have access to the system. Users are managed through the SailPoint application, which is part of the FDA enterprise Identity, Credential, and Access Management (ICAM) solution, and access is governed through Role-Based Access Control (RBAC) procedures. Users access the system exclusively through the internal FDA intranet using Single Sign-On (SSO) authentication via Personal Identity Verification (PIV) card. None of the URLs are publicly accessible. The production URLs are as follows: the CTP API Directory User Interface (UI) is accessible at https://dmpbc.fda.gov/ctp-api-directory/, ODGS is accessible at https://dmpbc.fda.gov/odgs/actuator/health, and the Appendix-A application is accessible at https://dmpbc.fda.gov/appendixa-web-ui/signon.
PTA 10:	Does the website have a posted privacy notice?	No
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	Yes

PTA 21A:	What are the AI tools and how are they used?	The CTP Data Modernization system utilizes artificial intelligence (AI) through ODT's Elsa API connection, an internal FDA system using Claude as the underlying model. HALO, which serves as the central data warehouse storing curated and trusted tobacco review and regulatory data, functions as the underlying data source that feeds into the Elsa AI system. Elsa leverages this curated data to provide intelligent, conversational query capabilities that allow authorized FDA users to interact with and retrieve tobacco review and regulatory data in a more intuitive way, rather than requiring users to manually construct complex GraphQL or Representational State Transfer (REST) API queries. As ODT's Elsa is an internal FDA system operating within the same agency and Operating Division, it is not considered a third-party website or application (TPWA). This functionality is supported by the Operational Data Gateway Service (ODGS), which provides a single, central point of access to multiple operational data sources using GraphQL technology, aligning with the AI model's need to fetch and synthesize data from multiple sources. HALO's role as a repository of curated and trusted data for business intelligence purposes and agency-wide data sharing initiatives provides the clean, structured data necessary to support reliable AI-driven responses. Elsa functions as an AI agent that draws upon HALO's data warehouse to respond to user queries, with the HALO data used in conjunction with the agents used in the FDA's Elsa API connections. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999

PIA 25:	For what primary purpose is the PII used?	The primary purpose for which PII is collected and maintained within the DMPBC system is to support the CTP regulatory review process. Specifically, the business PII collected, including business email addresses, business POC names, business phone numbers, and business mailing addresses, is used to facilitate communication with industry vendors who submit Premarket Tobacco or equivalent applications for product approval through FDA's CTP regulatory review process. This business PII enables FDA staff and authorized contractors to identify, contact, and correspond with the appropriate industry representatives throughout the regulatory review and approval process, including the submission, review, and disposition of Premarket Tobacco product applications. Additionally, the business PII is used to support the enterprise effort to standardize a global mailing address and a registration process for external vendor onboarding across FDA centers. HALO, as the central data warehouse under FDA's Intelligent Data Lifecycle Ecosystem (FiDLE), stores this PII in a curated and trusted format to ensure that it is readily accessible to authorized downstream systems, including CTP Rhapsody, CTP eSub, and the Center for Drug Evaluation and Research (CDER) Master Data Management (MDM) system, for the purposes described above. All downstream systems that have access to PII stored within HALO, including CDER MDM, are internal FDA systems operating within the same Operating Division under the Department of Health and Human Services (HHS), and therefore no PII is shared outside of the system's Operating Division.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There are no current secondary uses for the PII collected and maintained within the DMPBC system beyond the primary purpose described in PIA-25. The business PII collected is used solely to support the CTP regulatory review process and to facilitate communication with industry vendors who submit Premarket Tobacco or equivalent applications for product approval. The PII stored within the HALO central data warehouse is not used for testing, training, or research purposes. With respect to the system's use of AI through ODT's Elsa API connection using Claude as the underlying model, HALO data — including any PII stored therein — is used exclusively to respond to authorized user queries at runtime. HALO data is not used to train, fine-tune, or otherwise modify the underlying Claude AI model. The Elsa AI system retrieves and synthesizes data from HALO in response to specific user queries but does not retain, store, or repurpose that data beyond the scope of the individual query session. As such, the use of HALO data in support of the Elsa AI connection does not constitute a secondary use of PII and does not introduce any new categories of PII beyond those already described in PIA-22. In the event that any secondary uses for PII are identified in the future, including any uses related to the system's AI capabilities through ODT's Elsa API connection, the Privacy Impact Assessment (PIA) will be updated accordingly to reflect those uses and any associated privacy risks.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The following legal authorities govern information use and disclosure specific to the DMPBC system and program: The primary statutory authority for the collection and use of PII within the DMPBC system is the Family Smoking Prevention and Tobacco Control Act (Tobacco Control Act), Public Law 111-31, which grants the Food and Drug Administration (FDA) the authority to regulate the manufacture, distribution, and marketing of tobacco products, including the authority to require the submission of Premarket Tobacco product applications and associated business information from industry vendors. The Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. § 301 et seq., provides additional statutory authority for FDA's regulatory activities, including the collection and use of business PII in connection with the review and regulation of tobacco products. The Privacy Act of 1974, 5 U.S.C. § 552a, governs the collection, maintenance, use, and disclosure of PII by federal agencies, including the requirement to maintain accurate, relevant, timely, and complete records, and to provide individuals with the right to access and correct their records. The E-Government Act of 2002, Public Law 107-347, including the Federal Information Security Modernization Act (FISMA), Title III, governs the security and privacy of federal information systems, including the requirement to conduct Privacy Impact Assessments (PIAs) for systems that collect, maintain, or disseminate PII. The applicable Office of Management and Budget (OMB) information collection approval numbers governing this data collection are OMB Control No. 0910-0673 for FDA Form 3965b (expiration 04/30/2028) and OMB Control No. 0910-0879 for FDA Form 4057b (expiration 03/31/2028), issued pursuant to the Paperwork Reduction Act (PRA) of 1995, Public Law 104-13.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Non-Government Sources Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Control No. 0910-0673 for FDA form 3965b. Exp.04/30/2028 OMB Control No. 0910-0879 for FDA form 4057b. Exp. 03/31/2028
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	HALO is a data warehouse and not the source system; therefore, the method for notifying and obtaining consent from individuals whose PII will be collected is managed by the source system, eSub. The eSub system provides a banner notification to users at the point of data collection, warning them of the PII being collected prior to submission. This banner serves as the primary mechanism for notifying external regulated entities, such as industry vendors, that their non-sensitive business PII — including business email addresses, business Points of Contact (POC) names, business phone numbers, and business mailing addresses — will be collected, maintained, and shared as part of the Premarket Tobacco or equivalent application submission process through FDA's Center for Tobacco Products (CTP) regulatory review. To ensure that notification and consent mechanisms remain current and effective, the DMPBC system team coordinates with the eSub system team through established change management procedures. In the event that changes to the DMPBC system affect the collection, use, or disclosure of PII, the DMPBC system team notifies the eSub system team so that eSub's notification mechanisms can be reviewed and updated as appropriate. This coordination is documented through the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) review process, which ensures that any significant changes to the system's privacy posture are reviewed and approved by the appropriate FDA privacy officials prior to implementation. Additionally, the applicable Office of Management and Budget (OMB) information collection approval numbers governing this data collection — OMB Control No. 0910-0673 for FDA Form 3965b and OMB Control No. 0910-0879 for FDA Form 4057b — provide further notice to individuals of the PII being collected and the purpose for which it will be used.

PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	The process for notifying and obtaining consent from individuals whose PII is in the system when major changes occur is managed by the source system, eSub. In the event that major changes occur to the system, such as changes to disclosure practices or data uses, eSub would alert users of any changes to the PII collected through its notification mechanisms, including banner notifications presented to users at the point of data collection and submission. In the event that a major change occurs to the DMPBC system that affects the collection, use, or disclosure of PII, the change would be documented through the PTA and PIA review process. This process ensures that any significant changes to the system's privacy posture are reviewed and approved by the appropriate FDA privacy officials prior to implementation. The updated PIA would reflect any new or changed data uses or disclosures. To facilitate timely notification to affected individuals, the DMPBC system team maintains an active coordination relationship with the eSub system team. When a major change to the DMPBC system is identified that affects the collection, use, or disclosure of PII, the DMPBC system team formally notifies the eSub system team of the nature and scope of the change as part of the change management process. The eSub system team is then responsible for reviewing and updating its notification mechanisms — including banner notifications presented to users at the point of data collection — to ensure that affected individuals are informed of the change prior to or at the time the change takes effect. This inter-system coordination is documented in the system's change management records and reflected in the updated PTA/PIA submitted for FDA privacy official review and approval. It should be noted that HALO does not directly interface with end users and therefore cannot independently notify individuals of changes to the system. All user-facing notifications and consent processes are the responsibility of the source system, eSub, which serves as the primary point of contact between the system and external regulated entities such as industry vendors submitting Premarket Tobacco or equivalent applications for product approval through FDA's CTP regulatory review process.

PIA 36:	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 no process exists, explain why not.	The process for resolving an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, is primarily managed by the source system, eSub. HALO is a data warehouse and not the source system and therefore does not directly interface with end users. The eSub system maintains policies and procedures to work with user concerns regarding their PII, serving as the primary point of contact between the system and external regulated entities such as industry vendors submitting Premarket Tobacco or equivalent applications for product approval through FDA's CTP regulatory review process. In the event that an individual raises a concern regarding their PII, the individual would first contact the eSub system team, which would investigate the concern and take appropriate action to resolve it. If the concern involves PII that has been shared with or stored in HALO, the eSub system team would coordinate with the HALO system team to investigate and resolve the concern. Access to PII within HALO is governed through Role-Based Access Control (RBAC) procedures, which ensure that only authorized users and systems have access to the minimum amount of PII necessary to perform their functions. All downstream systems that have access to PII stored within HALO, including CTP Rhapsody, CTP eSub, and the CDER MDM system, are internal FDA systems operating within the same Operating Division under HHS and are held accountable for their own access controls through their individual Authorization to Operate (ATO) processes. Additionally, individuals may submit concerns or complaints regarding the handling of their PII to the FDA's privacy program through the FDA intranet, where privacy guidance and staff are available to assist. In the event that a privacy incident is identified, it would be reported and handled in accordance with FDA's established privacy incident response procedures and applicable federal regulations, including the Privacy Act of 1974.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The process for periodic reviews of PII contained in the system to ensure data integrity, availability, accuracy, and relevancy is primarily managed in coordination between the HALO system team and the source system, eSub. The following describes the processes in place for each element: Data Integrity: The integrity of PII stored within HALO is maintained through the system's adherence to Federal Information Security Modernization Act (FISMA) moderate controls under the Authorization to Operate (ATO) and System Security Plan (SSP) National Institute of Standards and Technology (NIST) controls. Access to PII within HALO is governed through Role-Based Access Control (RBAC) procedures, which ensure

that only authorized users and systems have access to the minimum amount of PII necessary to perform their functions. Databricks, which serves as the underlying storage platform for HALO, tracks all requests per system account, providing an auditable record of data access and modifications. The eSub system team is responsible for conducting periodic reviews of PII to ensure that the data stored in HALO accurately reflects the information provided by external regulated entities at the time of collection.

Data Availability: The availability of PII stored within HALO is maintained through the system's hosting infrastructure in FDA Amazon Web Services (AWS) GovCloud, which provides a highly available and resilient cloud environment. The system is categorized as a FISMA moderate impact system, with availability controls implemented in accordance with NIST Special Publication (SP) 800-53 to ensure that PII remains accessible to authorized users and systems when needed. The system's operational status is currently in the Operations and Maintenance phase, with ongoing monitoring and maintenance performed by the HALO system team to ensure continued availability.

Data Accuracy: The accuracy of PII stored within HALO is the responsibility of the source system, eSub, which serves as the primary point of collection for external regulated entity information, including business email addresses, business Points of Contact (POC) names, business phone numbers, and business mailing addresses. The eSub system team conducts periodic reviews of PII to ensure that the data stored in HALO accurately reflects the information provided by industry vendors as part of the Premarket Tobacco or equivalent application submission process through FDA's Center for Tobacco Products (CTP) regulatory review. In the event that an individual identifies inaccurate PII, they may contact the eSub system team to request a correction, which would then be reflected in HALO upon the next data refresh.

Data Relevancy: The relevancy of PII stored within HALO is ensured through the system's data governance processes, which are managed in coordination between the HALO and eSub system teams. As HALO is a data warehouse that stores curated and trusted data for business intelligence purposes and agency-wide data sharing initiatives, only PII that is necessary for the CTP regulatory review process and external vendor onboarding is collected and maintained. The enterprise effort to standardize a global mailing address and a registration process for external vendor onboarding further ensures that only relevant and necessary PII is collected and maintained within the system. Periodic reviews are conducted by the eSub system team to ensure that PII that is no longer relevant or necessary is identified and

		addressed in accordance with the retention guidelines established by the source systems.
PIA 38:	Identify who will have access to the PII in the system.	Users Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Internal FDA Users: Internal FDA employees with a valid FDA email address require access to PII in order to perform their designated functions in support of the Center for Tobacco Products (CTP) regulatory review process. This includes reviewing and processing Premarket Tobacco or equivalent applications submitted by industry vendors, as well as communicating with those vendors using the business PII collected and maintained within the system, including business email addresses, business Points of Contact (POC) names, business phone numbers, and business mailing addresses. Access is restricted to the minimum amount of PII necessary to perform their job functions, as governed through Role-Based Access Control (RBAC) procedures and managed through the SailPoint application, which is part of the FDA enterprise Identity, Credential, and Access Management (ICAM) solution. HHS/OpDiv Direct Contractors: Direct Contractors within CTP and other FDA centers require access to PII in order to support the development, maintenance, and operation of the DMPBC system and its associated data services in support of the CTP regulatory review process. Contractors are subject to the same RBAC procedures as internal FDA employees and are required to adhere to all applicable FDA privacy and security policies. All contractor access is governed through the system's active Authorization to Operate (ATO) and is limited to the minimum amount of PII necessary to perform their designated functions. Contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access Personally Identifiable Information (PII) within the DMPBC system are governed through a formal intake and access management process using Role-Based Access Control (RBAC) as the primary mechanism for controlling access. All system users, including internal FDA employees, HHS/OpDiv Direct Contractors, system administrators, and developers, must submit a formal access request that is reviewed and approved by the appropriate system administrators prior to being granted access to PII. Users are granted access only to the minimum amount of PII necessary to perform their designated job functions in support of the CTP regulatory review process, consistent with the principle of least privilege. User accounts and access privileges for both internal FDA employees and HHS/OpDiv Direct Contractors are managed through the SailPoint application, which is part of the FDA enterprise Identity, Credential, and Access Management (ICAM) solution, and access is authenticated via HHS/OpDiv Personal Identity Verification (PIV) card and Single Sign-On (SSO) through Active Directory (AD). All contractor access is additionally governed through the system's active ATO, and contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. All system users are required to complete mandatory FDA privacy and security training prior to being granted access to PII, and all access privileges are subject to periodic review to ensure that only authorized users retain access in accordance with the system's RBAC procedures and FISMA moderate controls under the ATO and SSP NIST controls. Any downstream systems are held accountable for their own access management procedures through their individual ATO processes.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	The DMPBC system employs several technical methods to ensure that those with access to PII are able to access only the minimum amount of information necessary to perform their job functions, consistent with the administrative procedures described in PIA-40. The primary technical method is RBAC, which is managed through the SailPoint application as part of the FDA enterprise ICAM solution and enforced across all components of the DMPBC system, including the HALO central data warehouse hosted in FDA AWS GovCloud. Access privileges are assigned based on a user's designated role and job function, ensuring that each user can only access the specific data and system functions necessary to perform their assigned responsibilities. The system includes a dedicated Identity and Access Management (IAM) Wrapper service that leverages the ODT enterprise platform to enforce access to queries and services, ensuring that only accounts with the correct privileges can access the ODGS queries and associated data. The Audit Logging Service (ALS) audits all events associated with usage of the IAM Wrapper service and records the results of security enforcement relative to requests to access ODGS queries, providing a comprehensive and auditable record of all data access events that enables system administrators to monitor and detect any unauthorized or inappropriate access to PII. Databricks, which serves as the underlying storage platform for HALO, enforces access controls at the data layer by providing a system account to each authorized system team and tracking all requests per system account. All users are required to authenticate via SSO using their HHS/OpDiv PIV card prior to accessing the system, ensuring that all access events are tied to a specific authenticated user account. Any downstream systems that have access to PII stored within HALO are held accountable for enforcing their own least-privilege access controls through their individual ATO processes and associated System Security Plans (SSPs), with all downstream system access tracked and logged through Databricks per system account. All technical access controls are implemented and maintained in accordance with FISMA moderate controls under the system's active ATO and NIST Special Publication (SP) 800-53 security control requirements.

PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users, including system owners, managers, operators, contractors, and program managers, are required to complete mandatory FDA privacy and security awareness training prior to being granted access to the DMPBC system and on an annual basis thereafter. This training is designed to make all system users aware of their responsibilities for protecting the Personally Identifiable Information (PII) being collected and maintained within the system. The mandatory training curriculum covers the proper handling, safeguarding, and disposal of PII in accordance with applicable federal laws and regulations, including the Privacy Act of 1974, the Federal Information Security Modernization Act (FISMA), and applicable National Institute of Standards and Technology (NIST) guidelines. These training requirements apply equally to internal FDA employees and HHS/OpDiv Direct Contractors who have access to the system. All users are additionally required to complete HHS-mandated information security and privacy awareness training, which provides foundational knowledge of federal information security and privacy requirements, including the proper handling of PII, the identification and reporting of privacy incidents, and the consequences of non-compliance with applicable privacy and security policies. System users are also assigned role-based security training commensurate with their designated role and level of access to PII within the system, ensuring that each user understands their specific responsibilities for protecting PII based on their assigned role and job function within the DMPBC system. All training completion is tracked and documented in accordance with FDA Staff Manual Guide (SMG) 3251.12 - Information System Security and Privacy Policy (IS2P), and access to the system may be revoked for any user who fails to complete required training within the designated timeframe.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is currently required for users of the DMPBC system beyond the general security and privacy awareness training. However, system users are provided with user guides and manuals that describe the specific functions and capabilities of the DMPBC system, including guidance on the proper handling and protection of PII within the system, which are designed to supplement the general security and privacy awareness training received by all users and provide system-specific context for applying privacy and security best practices. Privacy guidance and resources are also available to all system users through the FDA intranet, and FDA Privacy staff are available to provide guidance and answer questions related to privacy requirements and responsibilities. Additionally, given the system's integration of artificial intelligence (AI) through ODT's Elsa API connection using Claude as the underlying model, system users who interact with AI-driven components of the system are encouraged to consult with FDA Privacy staff and review applicable FDA AI governance guidance to ensure that their use of AI tools is consistent with applicable privacy requirements and best practices.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	HALO is not an original source of records; HALO is a central data warehouse that stores curated and trusted data sourced from upstream systems, including CTP eSub, which serves as the primary source system for external vendor submissions. As such, the retention guidelines for PII stored within HALO are managed by the source systems, and HALO does not independently set retention or destruction requirements for PII data. The CTP Electronic Submissions system, from which HALO sources its data, is managed according to multiple National Archives and Records Administration (NARA)-approved retention schedules based on record type. Adverse experience reports are governed by FDA file code 6132, consistent with NARA-approved schedule N1-88-07-2 for Adverse Experience Reporting System Database Records. Under this schedule, records are cut off annually at the end of the calendar year after a case is closed. The retention period is 30 years after cutoff, with provision for earlier destruction when no longer needed for trend analysis or reference purposes, as approved by FDA Records Management. Records are destroyed in accordance with NARA-approved methods for electronic records containing PII. Tobacco product submissions, including registration, product listing, ingredient listings, and premarket applications, are governed by records schedule DAA-0088-2020-0001. Records are cut off at the end of the calendar year after final determination has been taken or the product has been taken off the market, whichever is later. The retention period is 30 years after cutoff. Records

		are destroyed in accordance with NARA-approved methods for electronic records containing PII. Contact information for tobacco industry representatives, including the business email addresses, business Points of Contact (POC) names, business phone numbers, and business mailing addresses collected and maintained within the DMPBC system, is retained for the duration of the associated regulatory matter plus seven years after the regulatory matter is closed or the product is removed from the market, whichever is later, consistent with FDA's general administrative records retention practices. This retention practice is applied pending the formal assignment of a NARA-approved records schedule specific to this category of industry contact records. Until a formal schedule is assigned and approved by NARA, these records are treated as temporary records and retained in accordance with FDA records management policies, as described in the final paragraph of this section. Contact information is also retained until superseded by updated information provided through subsequent submissions. Outdated contact information that is no longer accurate or necessary is removed during quarterly data quality reviews to minimize retention of unnecessary PII. Upon reaching the end of the retention period, industry contact information is destroyed in accordance with NARA-approved methods for electronic records containing PII. Until all formal file code assignments are complete, records not covered by an approved schedule are retained in accordance with FDA records management policies as temporary records, pending NARA approval of appropriate retention schedules. All records are protected by the administrative, technical, and physical safeguards described throughout this Privacy Impact Assessment (PIA) during their entire lifecycle, including during retention and destruction, in accordance with Federal Information Security Modernization Act (FISMA) moderate controls under the system's active Authorization to Operate (ATO) and System Security Plan (SSP) National Institute of Standards and Technology (NIST) controls.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	The DMPBC system secures Personally Identifiable Information (PII) through a comprehensive set of administrative, technical, and physical controls implemented in accordance with FISMA moderate controls under the system's active ATO and applicable NIST Special Publication (SP) 800-53 security control requirements. The following describes the controls in place for each element: Administrative Controls: All system users, including internal FDA employees, HHS/OpDiv Direct Contractors, system administrators, and developers, are required to complete mandatory FDA privacy and security awareness training prior

to being granted access to the system and on an annual basis thereafter. Access to PII within the DMPBC system is governed through a formal intake and access management process using Role-Based Access Control (RBAC) as the primary mechanism for controlling access, ensuring that each user is granted only the minimum amount of access necessary to perform their designated job functions. Contracts with HHS/OpDiv Direct Contractors include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. All access privileges are subject to periodic review to ensure that only authorized users retain access to PII within the system, and access may be revoked for any user who fails to comply with applicable privacy and security policies or who no longer requires access to perform their job functions.

Technical Controls: The primary technical control used to enforce least-privilege access to PII within the DMPBC system is RBAC, which is managed through the SailPoint application as part of the FDA enterprise Identity, Credential, and Access Management (ICAM) solution. The system includes a dedicated Identity and Access Management (IAM) Wrapper service that leverages the ODT enterprise platform to enforce access to queries and services, ensuring that only accounts with the correct privileges can access the Operational Data Gateway Service (ODGS) queries and associated data. The Audit Logging Service (ALS) audits all events associated with usage of the IAM Wrapper service and records the results of security enforcement relative to requests to access ODGS queries, providing a comprehensive and auditable record of all data access events. Databricks, which serves as the underlying storage platform for the HALO central data warehouse, enforces access controls at the data layer by providing a system account to each authorized system team and tracking all requests per system account. All users are required to authenticate via Single Sign-On (SSO) using their HHS/OpDiv Personal Identity Verification (PIV) card prior to accessing the system, ensuring that all access events are tied to a specific authenticated user account. All data is encrypted in transit and at rest in accordance with FISMA moderate controls and applicable NIST security standards, and the system is hosted in FDA Amazon Web Services (AWS) GovCloud, which provides a highly secure and compliant cloud environment for the storage and processing of sensitive government data.

Physical Controls: The DMPBC system is hosted entirely within FDA AWS GovCloud, a Federal Risk and Authorization Management Program (FedRAMP) -authorized cloud environment that provides robust physical security controls for the protection of government data. Physical access to the underlying infrastructure supporting the DMPBC system is restricted to authorized AWS personnel and is governed by AWS's physical security controls, which include multi-factor

		authentication, video surveillance, and security personnel at all data center facilities. As a cloud-hosted system, the DMPBC system does not maintain any on-premises hardware or physical infrastructure that would require additional physical security controls beyond those provided by the FDA AWS GovCloud environment. All physical security controls are implemented and maintained in accordance with FISMA moderate controls under the system's active ATO and applicable NIST SP 800-53 security control requirements.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/15/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/22/2026
SOP Review Comments:		**# of Days - SOP Review:**	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/24/2026
Agency Privacy Analyst Review Comments:	Reviewer: Philomina Dorkenoo 6/24/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	2

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/2/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/2/2026 2:36 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	6/23/2026	6/23/2026 Per FDA Email: The PIA is experiencing an Archer error with Question #3 of the general information section. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is 8/20/2024. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	