PTA / PIA: OS - FedHub - QTR3 - 2025 - OS3059608

Created Date: 9/26/2025 1:11 PM Last Updated: 11/24/2025 4:02 PM

General Information

PTA / PIA Name:	OS - FedHub - QTR3 - 2025 - OS3059608	**PTA / PIA ID:**	3869920
Component Name:	OS - FedHub	**ATO Boundary Name:**	FedHub
Overall Status:	Complete	**# of Days - Open:**	89
Submitter:		**Submit Date:**	9/18/2025
Next Assessment Date:	11/23/2028	**Expiration Date:**	11/23/2028
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
General 02:	Is this a FISMA-Reportable system?	No
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.	11/28/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Joy Chapman
PTA 01A:	POC Title and Organization	System Owner, Program Support Center
PTA 01B:	POC Email Address	Joy.Chapman@hhs.gov
PTA 01C:	POC Phone Number	301-348-3315
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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 Department of Health and Human Services (HHS) FedHub system provides federated authentication services for external users (cross-government agency users, citizens, local, and state). The HHS FedHub system incorporates the existing HHS NextGen XMS architecture and integrates with the United States Office of Management and Budget (OMB) Max.gov authentication portal. The HHS FedHub system contains additional federation capabilities and replaces the MAX authentication portion of the existing Max.gov system. HHS FedHub system leverages credentials issued by credential service providers (CSPs) or via an agency issued Personal Identity Verification (PIV)/Common Access Card (CAC). The solution also includes capabilities that meet identity proofing and multi-factor authentication (MFA) requirements. Additional credential service providers will be added after the system goes into production. Current CSPs include General Services Administration's (GSA's) Login.gov and ID.me. An Interagency Agreement (IAA) is in place for Login.gov at the Department Level and for ID.me.

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.	**Personal Identity and Authentication**-- this value is passed to FedHub from Login.gov or ID.me and is not stored. Data shared includes: Business/academic/official email address: e.g., .edu, .com, .org domain. User ID: FedHub unique ID (XID) used to identify a user account Universally unique identifier (UUID) & credential identifier (CID): values offered by credential service providers (CSPs). **Personal Identity Verification (PIV)/Common Access Card (PIV/CAC) card attributes:** All PIV information is stored for the lifetime of the credential and is automatically removed by the system when the credential is either expired or manually removed by the user. It is also removed if the user account is inactive for 13 months or through an account deletion request. Federal Agency Smart Credential Number (FASC-N)): identifier issued as attribute on PIV card. Electronic Data Interchange Personal Identifier (EDIPI): identified issued as attribute on CAC card. Universal Principal Name (UPN): alternate identified issues as attribute on PIV/CAC. Note: Format dependent on issuing agency. First Name: e.g., John -– this value is provided either upon completion of identity proofing with the third-party identity proofing provider or pulled from a federal agency PIV/CAC. Middle Name (if applicable): e.g., Stephen - this value is provided either upon completion of identity proofing with the third-party identity proofing provider or pulled from a federal agency PIV/CAC card. Last Name: e.g., Doe - this value is provided either upon completion of identity proofing with the third-party identity proofing provider or pulled from a federal agency PIV/CAC card. Request information including User ID, Registration Email, Email, User-App ID, Request ID, Requestor ID, Approver ID, and ID. Application Names: Provided by the HHS Operating Division (OpDiv) Organization Names: , e.g., pharmaceuticals; universities - provided by the end user as part of organization registration process. SSN, truncate SSN, drivers license Number, Passport Number, Employment Status/History, Military Status/History, Photographic Identifiers, Medical Records Number, Patient ID Number. The FedHub component does not issue or maintain credentials for any users. This is handled by Login.gov and ID.me. Note: users are defined as external federal government and non-government users. Direct contractors are considered internal user population and therefore would not use FedHub for authentication and access.
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.	Login.gov Username/password ID.me Username/password HSPD-12 PIV or CAC card
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.	**Personal Identity and Authentication attributes (UserID, UUID, CID, and email):** This information is collected and shared between FedHub and the credential service providers (CSPs) login.gov and ID.me and is used for authentication and authorization purposes to ensure authorized users can access the necessary integrated federal applications. This information is shared only and is not stored by the system for longer than the authorization session. **Personal Identity Verification (PIV)/Common Access Card (PIV/CAC) card attributes:** This information is collected and shared between FedHub and the credential service providers (CSPs) login.gov and ID.me and is used for authentication and authorization purposes to ensure authorized users can access the necessary integrated federal applications. This information is shared only and is not stored by the system for longer than the authorization session. **Categories of Individual:** Business Partners/Contacts (Federal state, local agencies): These individuals are general users of the system. Information collected will include Personal Identity and Authentication attributes (UserID, UUID, CID, and email) and Personal Identity Verification (PIV)/Common Access Card (PIV/CAC) card attributes. Employees/HHS Direct Contractors: These individuals are privileged/non-privileged users of the system. Information collected will include Personal Identity and Authentication attributes (UserID, UUID, CID, and email) and Personal Identity Verification (PIV)/Common Access Card (PIV/CAC) card attributes
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).	FedHub.gov will be the primary URL with FedHub.hhs.gov as a back-up.
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

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.	FedHub will be the authentication portion only. Purpose: The purpose of FedHub will be to provide authentication. User types: Users accessing FedHub will include internal and external federal government users and non-government users (citizens, local, and state). Accessibility: Users will access the system through the public URL and then use their credential via Login.gov or ID.me to access their permitted federal resources.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
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?	Yes
PTA 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS
PTA 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	Mobile application is accessible to HHS citizens, local, state, and other non-HHS external users who have a need to access an HHS application and can sign in to that application leveraging methods integrated with FedHub such as Login.gov and/or ID.me. FedHub integrates with sign in partners that meets identity proofing and various HHS and federal requirements (e.g., NIST 800-63).
PTA 16:	Does the mobile application have a privacy notice?	Yes
PTA 17:	Does the mobile application contain links to non-federal government websites external to HHS?	Yes
PTA 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	Yes
PTA 18:	Does the mobile application use measurement and customization technology?	Yes
PTA 18A:	Describe the type(s) of measurement and customization technologies or techniques in use in the mobile application and what information is collected.	Web development tool is used to create FedHub component mobile device interfaces compatible with Apple Mobile operating system (iOS), android, tablets, and laptops.
PTA 19:	Does the mobile application have any information directed at children under the age of thirteen?	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?	No

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.	Identifying Numbers Social Security Number Truncated SSN Driver's License Number Passport Number Employee ID Number Device Identifiers Biographical Information Name Date of Birth User Credentials Certificates (e.g., training certificates) Employment Status/History Military Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Biometrics/Distinguishing Features Photographic Identifiers Medical Information Medical Records Number Patient ID Number Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	User ID: FedHub unique ID, Universally unique identifier (UUID) & credential identifier (CID) Personal Identity Verification (PIV)/Common Access Card (PIV/CAC), User-App ID, Request ID, Requestor ID, Approver ID, ID, Organization Names, IP address, Device attributes.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999

PIA 25:	For what primary purpose is the PII used?	The primary purpose of PII use is for user authentication and authorization and is used to ensure authorized users can access the necessary integrated federal applications.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	No secondary uses of PII.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	The Social Security Number (SSN) is provided by the individual to FedHub but it is not stored in the system. Instead, the SSN is passed to the third-party identity proofing provider (e.g., ID.me/Login.gov/Other Credential Service Provider) so they can verify that the person using the credential from Login.gov is actually who they say they are.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	Per federal government application needs, the SSN/Taxpayer ID attributes will be a pass through to verify individual identification. The implementation of this system, including activities such as the collection of Personally Identifiable Information (PII) necessary for operating it, are authorized by 5 U.S.C. 301, which authorizes the Secretary to create regulations necessary for meeting the missions of his or her agency. While SSN is not stored in the database, the SSN is temporarily in the application for a short period of time until authentication is completed (in alignment with E.O. 9397).
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301, which authorizes the Secretary to create regulations necessary for meeting the missions of his or her agency. Further, 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to maintaining the infrastructure of the agency.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Name, Email, FASC-N, EDIPI, XID (Unique Identification), Organization, Application Name, XMS uses the listed data elements to validate the external user's account credentials from Login.gov or other Credential Service Providers (CSP) and verifies the identity of that external user.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-0777 Facility and Resource Access Control Records SORN history: 75 FR 47812 (8/9/10), *83 FR6591 (2/14/18)

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	N/A
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	**Other Federal Agency/Agencies**: PII is shared for user identification and authentication only and is passed through from the CSPs to FedHub. This group will encompass external users of the tool. Users will not have direct access to PII that is not their own. **State or Local Agency/Agencies:** PII is shared for user identification and authentication only and is passed through from the CSPs to FedHub. This group will encompass external users of the tool. Users will not have direct access to PII that is not their own. **Within HHS:** This group is a small subset of internal HHS users and direct HHS contractors. PII is disclosed for account management purposes only.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	FedHub is a new system. By go-live, connections will be Interagency Agreements (IAA) with credential service providers General Service Administration (GSA) Login.gov and ID.me. Interconnection Security Agreements and Memorandums of Understanding for OpenID Connect or SAML integrations will be drafted and prepared after go-live for relying party applications which will integrate with FedHub.

PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	FedHub will be logging & auditing the sharing of PII with integrated applications. The only location of PII within logging and auditing will be in the logs containing Security Assertion Markup Language (SAML) Responses received from Credential Service Providers who are providing PII (at this time, only Login.gov and ID.me) and the logs containing SAML Assertions sent from XMS to Relying Parties containing PII. These logs will be initially created on the designated servers and then archived for the duration of our retention policy, all within our Amazon Web Services (AWS) environment.
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.	When attempting to create an account or authenticate, the user will be prompted for the HHS Privacy Policy and Terms of Use. Selecting 'Deny' will decline the collection and use of data. The user will not be able to continue forward with account registration or authenticate into an application without accepting the HHS Privacy Policy and Terms of Use. Additionally, users may cancel out of the account registration workflow or authentication workflow. If canceled, the user will not be able to continue forward with registration and must begin a new user session.
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.	User will be notified via email address provided to FedHub of any subsequent changes to FedHub, Login.gov or ID.me where their profile and/or PII are impacted (such as being shared with a system). Users can submit a request directly to FedHub via email in the event they do not consent to changes implemented. Specific to adaptive authentication, stakeholders will be notified prior to adaptive authentication go live. No existing profiles will be impacted. Post-adaptive authentication go live, attributes will begin to be collected from users by the adaptive authentication service as they interact with FedHub.
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.	There is a link to the HHS Privacy Policy embedded on all pages within FedHub for the users to access to address any concerns as it relates to PII issues.
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.	FedHub will receive PII via Credentialed Service Providers or Alternative Authentications (FIDO (Fast IDentity Online) or PIV/CAC Card) and will periodically update data when a user accesses the system. Users can validate and update their data themselves directly with Credentialed Service Providers.
PIA 38:	Identify who will have access to the PII in the system.	Administrators 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.	Administrators: for operations and maintenance of the system. Sensitive PII is not stored in FedHub. Administrators will access data to manage user account access. Contractors: For purposes of FedHub, all contractors support functionality of the FedHub system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only admins tasked with management responsibilities with respect to the production database have access to PII. These admins are vetted during the project onboarding process, and the access may only be provisioned once requested and explicitly approved by a team lead. These requests for access provisioning and deprovisioning are maintained to provide an auditable trail of admin access and the need that was presented to obtain it.
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.	Segregation of duties is enforced to ensure that only users with the System Administrator role are able to access the backend database that stores the First Name, Middle Name, Last Name, Email Address, and Organization attributes. FedHub utilizes an encrypted database to store PII data at rest. This information is only accessible by administrators that have been provisioned with the needed access permissions.
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 Administrators must attend and complete all applicable federal privacy training annually including Privacy Awareness Training, Security Awareness Training, and Role-based Training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Internal system training is available via role-based trainings on security procedures to ensure personnel are adequately aware of security and privacy requirements.
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).	Records are retained in accordance with General Records Schedule 3.2: Information Systems Security Records Item 30. Disposition Authority: DAA-GRS- 2013-0006-0004. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

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.	All applicable NIST 800-53 Moderate baseline controls implemented within FedHub Implementation response statements will be covered documented in Appendix X of FedHub System Security Plan (SSP). These controls include, but are not limited to the following: Administrative Controls: System security plan Contingency Plan File backup Security Awareness and Training Contractor Agreements Least Privilege Access Technical Controls: User Identification Passwords Firewall Virtual Private Network Encryption Intrusion Detection System Physical Controls: Guards Identification Badges Key Cards Cipher Locks Biometrics Closed Circuit TV Biometric data is not being captured or stored in FedHub. The use of biometric data is in context for the physical controls that are used by the vendor in managing access to the Amazon Web Services (AWS) GovCloud and Federal Risk and Authorization Management Program (FedRAMP) approved data center where FedHub is hosted.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/22/2025
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	4

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/26/2025
SOP Review Comments:		**# of Days - SOP Review:**	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/20/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/20/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	55

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/24/2025 2:37 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 05	Data Feed Service, pta_pia_OS_Release	9/8/2025	Please include the length of time the Personal Identity information will be stored.	

			Please reformat response so that it does not use bullet points, as they are not 508 compliant.
PTA 06	Data Feed Service, pta_pia_OS_Release	9/8/2025	Please indicate the category of individual(s) that the information is collected about. (e.g. Employees, Members of the Public, etc.) Please also indicate if the information is shared in any way.
PIA 26	Data Feed Service, pta_pia_OS_Release	9/9/2025	Is adaptive authentication using AI? If so, please indicate in response and change response to the related PTA question (PTA-21) to a 'yes'. As PII is being used for a secondary purpose, please complete and submit the Privacy Risk Analysis Checklist provided (attached to the PIA submission in the 'supporting documents' section. Once completed, please submit it to the OS Privacy Inbox (osprivacymaibox@hhs.gov) upon re-submission of the PIA.
PIA 32B	Data Feed Service, pta_pia_OS_Release	9/9/2025	This response should be rewritten to include: For each type selected in PIA 32A: • Name or describe the entities or individuals that have direct access to or receive PII directly from the system; and • Explain why and for what purpose PII is shared with each entity or individual.
PIA 32D	Data Feed Service, pta_pia_OS_Release	9/9/2025	Another response in the PIA indicates that there will be a backend database that is storing information, contrary to what is listed in this response: 'Segregation of duties is enforced to ensure that only users with the System Administrator role are able to access the backend database that stores the First Name, Middle Name, Last Name, Email Address, and Organization attributes.' Please adjust either response to fix this discrepancy.
PIA 22	Data Feed Service, pta_pia_OS_Release	9/9/2025	Please select the 'other' option and include the following information: User ID: FedHub unique ID, Universally unique identifier (UUID) & credential identifier (CID) Personal Identity Verification

			(PIV)/Common Access Card (PIV/CAC), User-App ID, Request ID, Requestor ID, Approver ID, ID, Organization Names, IP address, Device attributes. Additionally, the follow fields are selected but not listed as being collected in PTA-5: SSN, truncate SSN, drivers license Number, Passport Number, Employment Status/History, Military Status/History, Photographic Identifiers, Medical Records Number, Patient ID Number. Please update the response of PTA-5 to include the information selected.
PTA 08A	VILLAFUERTE, NESTOR	10/7/2025	Is the website already published? Reviewer notes that both URLs provided were unreachable at the time of review.
PTA 08A	BLAND, CRYSTAL	11/20/2025	The system is New and haven't went live yet. That is why the URL is unreachable.