PTA / PIA: HRSA - HDF - QTR3 - 2025 - HRSA1446283

Created Date: 8/14/2025 12:21 PM Last Updated: 8/29/2025 4:21 PM

General Information

PTA / PIA Name:	HRSA - HDF - QTR3 - 2025 - HRSA1446283	**PTA / PIA ID:**	3649622
Component Name:	HRSA - HRSA DocuSign Forms	**ATO Boundary Name:**	DocuSign
Overall Status:	Complete	**# of Days - Open:**	49
Submitter:		**Submit Date:**	7/11/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**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.	7/22/2024
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	Michael Makinde Rebecca Andam
PTA 01A:	POC Title and Organization	ISSO, HRSA
PTA 01B:	POC Email Address	MMakinde@hrsa.gov
PTA 01C:	POC Phone Number	301-370-9562
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes since last PTA

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.	DocuSign is a San Francisco- and Seattle-based company that provides electronic signature technology and Digital Transaction Management services to facilitate electronic exchanges of contracts and signed documents. DocuSign's features include authentication services, user identity management, and work flow automation. Signatures processed by DocuSign are comparable to traditional signatures based on the product's compliance with the ESIGN Act as well as the European Union's Directive 1999/93/EC on electronic signatures. The DocuSign application is used by the Human Resource Program to facilitate the paperless submission of application forms through the on-boarding employee process.
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.	DocuSign only targets PII data fields related to the agency customer's technical administrator during the deployment phase of the DocuSign Federal system for an agency customer. This data field is targeted to collect and store PII of name, physical address, and email address for the technical administrator who acts as the point-of-contact (POC) within the agency customer's organization. DocuSign collects SSN, Name, Date of Birth, E-mail address, Mail address, Phone Numbers and Military Status
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.	HRSA OKTA with HRSA AD
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.	DocuSign Federal is a SaaS application oriented towards federal government entities. Operated and managed as a government community cloud, DocuSign Federal provides government customers with an enterprise signing service to facilitate paperless work flow management. More information about DocuSign Federal can be found here: www.docusign.com. The Human Resource office uses the DocuSign tool to collect PII approved by the OMB No. 3206-0182 form such as SSN, Name, Date of Birth, E-mail address, Mail address, Phone Numbers and Military Status
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).	Production: https://account.docusign.com QA: https://account-d.docusign.com

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.	HRSA DocuSign Forms (HDF) is an electronic signature application that HRSA uses to have electronic forms filled out and signed by various HRSA business programs. HDF leverages the DocuSign FedRAMP authorized application. HRSA utilizes HDF to automate self-service signing of Office of Personal Management (OPM) approved forms. The system is accessible to about 90 internal users from HRSA Personnel Security Signing Group and key bureaus/offices like BPHC, BHW, HSB, PRB etc. The forms are made available by the HRSA DocuSign internal users via emailing a secure DocuSign PowerForm link. HDF generates and emails an individualized validation code to the secure link recipients. Secure link recipients access the forms through the provided link after entering the validation code. The forms can only be signed by the secure link recipients. Additionally, the forms can only be signed through the provided secure PowerForm link. DocuSign administrators leverage Access Management System (AMS) to authenticate and manage the HDF application. Secure link recipients can only access the forms through the PowerForm link. HDF maintains a full audit trail of all form transactions. HDF records a complete summary of envelope (email) events, signer events, including the signer's IP address and other identifying information, signature image, and key event timestamps. The following are the forms managed by HDF: • OF-306 onboarding form for new hires coming into HRSA. • HHS 745 Form for badge renewal. • Cybersecurity Awareness Training Certificate completion form. • Cybersecurity Awareness Admin Training Certificate completion form.
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?	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?	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 Biographical Information Name Date of Birth Military Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/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 PII information collected by the DocuSign tool used by the Human Resource Program facilitate the on-boarding employee process.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	DocuSign does not use PII for testing training or research
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.	SSN is collect but not used by DocuSign application tool.
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.	Executive Order 9397 numbering system for federal accounts relating to individual persons. Citation: E.O. 9397
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Executive Order 9397 numbering system for federal accounts relating to individual persons.
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
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.	OPM GOVT-1 OPM/GOVT–2
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online
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 No. 3206-0182
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.	When an new employee subscribes to the DocuSign Federal system, the new employee is consenting to the collection and use of their information. Noted in DocuSign Privacy Policy.
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.	When an new employee subscribes to the DocuSign Federal system, the new employee is consenting to the collection and use of their information. Noted in DocuSign Privacy Policy.
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 no process, as individuals are notified at the time they submit the information stored in DocuSign that it will be used for legitimate purposes and it will not be disclosed unless authorized by law.
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.	Annual updates used to maintain accuracy of data.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	USERS: Users have access to PII as part of the hiring process data collection ADMINISTRATOR: DocuSign provides limited PII-level access to DocuSign personnel authorized to access the DocuSign Federal system for operational, maintenance, security, and customer support purposes. DocuSign roles that have access to the DocuSign Federal system include Product Security, Security Operations, Technical Operations, and Customer Support. DocuSign personnel only have access to PII relating to eDocument transactional information for customer support purposes.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	DocuSign Federal employs multiple mechanism to prevent the misuse of PII by those having access. The only accessible PII information is eDocument transaction records which include information regarding the sender and recipients (name and email address). This eDocument transaction record is only accessible by DocuSign Customer Support staff (administrator) who are given the eDocument Transaction ID by the HRSA Human Resources system owner . All PII information within a DocuSign Envelope (eDocument) is encrypted with DocuSign staff not having physical or logical access

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.	DocuSign provides limited PII-level access to DocuSign personnel authorized to access the DocuSign Federal system for operational, maintenance, security, and customer support purposes. DocuSign roles that have access to the DocuSign Federal system include Product Security, Security Operations, Technical Operations, and Customer Support. DocuSign personnel only have access to PII relating to eDocument transactional information for customer support purposes.
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.	DocuSign requires all DocuSign personnel to undergo annual awareness and security training (including privacy training) upon hire before personnel are granted access to the DocuSign Federal system. Additionally, DocuSign provides annual awareness and security training to all DocuSign personnel. DocuSign requires contractors to undergo the same training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System users receive training related to their job responsibilities in addition to security and privacy awareness training. Security and privacy awareness training is conducted annually. Job training is provided as needed.
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).	DocuSign establishes retention periods for PII within the DocuSign Federal system. PII within DocuSign envelopes and envelope-transactional data is stored as long there is a business purpose within the system for audit, legal, and customer use. HRSA Human Resources system owner have the capability to configure their own record retention policy within the system in order to control the defined time frame of purging data from their account.
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.	HRSA Human Resources system data associated with DocuSign Federal system is considered restricted, confidential, and sensitive, in accordance with DocuSign information classification standards. DocuSign Federal provides consistent information flow protections for all customer data permitted within DocuSign Federal, regardless of sensitivity level. Federal user entities are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them. For HRSA Human Resources users signing or reviewing of documents hosted within DocuSign Federal, an email is generated by the customer, which includes unique and time sensitive links back to DocuSign Federal production web-servers that allow the customer client to securely review and sign the respective document. All customer documents and supporting data are securely retained for the lifetime of the document.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/14/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	3

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/14/2025
SOP Review Comments:		**# of Days - SOP Review:**	31

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	8/20/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 8/20/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/29/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	9

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/29/2025 1:34 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
PIA 22	BLAND, CRYSTAL	8/20/2025	On the next iteration of the PIA please include "Email address (Business)" of the Administrator of the customer's organization that act as a POC, per PTA-5.	