Privacy Impact Assessment for the VA IT System called:

DOCUSIGN FEDERAL -ENTERPRISE

VACO

TECHNOLOGY AND PLATFORM SERVICES

Date PIA submitted for review:

7/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Yentl Brooks	Yentl.Brooks@va.gov	(713) 383-1879
Information System Owner	April Primous	April.Primous@va.gov	512-326-7862

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

DocuSign enables veterans and their surrogates to digitally sign forms that require a high level of verification that the user signing the document is a legitimate and authorized user. In addition, DocuSign provides a mechanism for VA applications to verify the authenticity of user documents and data integrity on user forms.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

DocuSign -Enterprise Software as a Service (SaaS), Technology and Platform Services (TPS), Office of Information and Technology (OIT), Infrastructure Operations (IO), Application hosting, Cloud and Edge Solutions (ACES)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

DocuSign -E is used by Technology and Platform Services (TPS) as an eSignature (eSig) service for VA use. This service is supported by the SaaS Solution of DocuSign and also aligns with OIT Digital Transformation, Priority 3: Business Transformation, OIT Enterprise Roadmap (2018-2024), OIT Transformation, Technology Business Management. The VA DocuSign -E eSignature (eSig) program office owns the DocuSign SaaS Solution. The purpose of DocuSign is to allow clients, or end users, to create a digital analog to a wet signature, and apply that signature to digitized documents. Also, the purpose is to allow customers, or direct consumers of the DocuSign services, to upload a document or form, assign areas within a document or form for a client to apply their applicable digital signature, and to utilize that signed document to fulfill the specific mission of the customer. 100,000+ users are expected to use DocuSign. It will be used in tangent with eSig. DocuSign needs the eSig service as that ensures users are authenticated and application meet the VA requirements for non-repudiation. The estimated users of DocuSign could be in the millions of personnel, as it will be agency personnel requesting signatures from veterans on a variety of forms. There is no exact count of whom may log in, but the permissions are set within DocuSign that allow the customer to dictate exactly one person to sign a form, and that one person can only sign that form and not access other forms stored within DocuSign. Beginning with the Government Paperwork Elimination Act of 1998 (GPEA), the Federal government has encouraged the use of electronic / digital signatures to enable electronic transactions with agencies, while still providing a means for proof of user consent and non-repudiation. To support this capability, some means of reliable user identity management must exist.

C. Indicate the ownership or control of the IT system or project.

VA Partnership

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The estimated users of DocuSign could be in the millions of personnel, as it will be agency personnel requesting signatures from veterans on a variety of forms. There is no exact count of whom may log in, but the permissions are set within DocuSign that allow the customer to dictate exactly one person to sign a form, and that one person can only sign that form and not access other forms stored within DocuSign. Signers who are not part of the VA do not get or need an account in the VA DocuSign -E to sign VA documents sent to them to obtain an electronic signature.

E. A general description of the information in the IT system and the purpose for collecting this information.

DocuSign -Enterprise Software as a Service (SaaS) – Information collected is based on the type of document sent to a recipient for eSignature purpose. See section 1.1 for a list of information which may be collected by any one of our VA business lines. The reason for collecting this information would be for use with that business line's purpose based on the document being requested to sign.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

This capability is enabled by the eSig service. The eSig service signing process includes the following steps: 1. Form Signing Attestation: The user affirms their intent to electronically sign the document and understands re-authentication is part of that process. 2.Re-Authentication: The user must refresh their authentication by repeating the authentication process, which is to connect through the appropriate SSOi or SSOe interface, log in with approved credentials. This re-authentication phase uses the Cloud Service Provider (CSP) from the current authenticated session to initiate a quicker login process and return to the application. 3.Form Signing: The eSig service is used to add a digital signature to the form. 4. Form Storage: The signed form must be stored for later validation. In this process, the application is entirely responsible for steps 1, 2, and 4. Applications use the capabilities within Access VA to support the Attestation and Re-Authentication phases with full page and widget modes. In step 3, the application must use the eSig service to send the form for signing and retrieve the signed form. • If the forms stored on DocuSign were to be compromised or otherwise disclosed intentionally or unintentionally, the loss of privacy of the data on the forms, which can include PHI, PII and Financial data, would significantly harm the reputation of the Credential Service Providers, and to the VA. • SSO-e or VAAFI, a component of Identity Access Management does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by SSOe comes from Credential Service Providers (IAM) external to the system. No databases are involved with storing or sharing of the information. The Sending VA department is responsible for the completed signed document and how it is shared within or outside their organization or where this completed signed documents are stored. The information which may be requested and stored by the VA business line are: Name, Full SSN, DOB, Mothers maiden name, personal mailing address, personal phone

numbers, personal email address, financial account information, certificate/license numbers, IP address, race/ethnicity, Tax ID number full name, Medications, Patient ID, medical records

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

There is one instance of DocuSign -Enterprise Software as a Service (SaaS)

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The following is a full list of related laws, regulations and policies and the legal authorities: NIST Special Publication 800-63 Version 1.0.2; Electronic Authentication Guideline OASIS XACML 2.0 Section 508 Standards Guide VA Directive 6500; Information Security Program VA Directive 6501; VA Identity Verification OMB 04-04 E-Authentication Guidance for Federal Agencies Aligns with the VA Enterprise Shared Services directive and strategy Supports HSPD-12 specifications where applicable (i.e., Personal Identification Verification (PIV)) Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397. The SORNs that are relevant are VA SORNs. Those include: 145VA005Q3 (Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA); 146VA005Q3 (Department of Veterans Affairs Identity Management System (VAIDMS)-VA); 150VA19 (Administrative Data Repository-VA); 121VA10 (National Patient Databases-VA); 138VA005Q (Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA); 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records - VA); 58VA21/22/28 (Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA)

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The system is not in the process of being modified.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No changes in business processes because of this PIA

K. Whether the completion of this PIA could potentially result in technology changes

No new technology changes will result with this PIA.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Due to the nature of DocuSign, there are unknowns to the types of data that may be on forms that are uploaded to DocuSign. Generally, a VA office will request an employee, veteran using their Patient ID, external entity such as DoD healthcare offices, or non-VA patient provider to sign a document.

DocuSign does not utilize, read in, or is aware of any of the information on any of the forms, however as the document will reside on the DocuSign service until it is downloaded, which is what poses the privacy risk.

PII Mapping of Components (Servers/Database)

DocuSign consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DocuSign and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database Server Tier	No	Yes	Any PII entered into the DocuSign application by the customer	Customer account management, web transactions	All measures stated in the FedRAMP moderate baseline including access management, security monitoring/logging, alerting and incident response
NAS Storage Tier	No	Yes	Any PII entered into DocuSign documents by the customer.	Customer data storage and retrieval	All measures stated in the FedRAMP moderate baseline including access management, security monitoring/logging, alerting and incident response

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information sources for DocuSign are for VA offices that utilize the eSig (DocuSign) service. This includes the following partners that currently use the eSig (DocuSign) service.• VHA eHealth Exchange (Nationwide Health)• VBA eBenefits .The information will come from the source partner in terms of information on the forms that need to be signed by a requested signee. This information could include healthcare information and privacy act information from eHealth Exchange; Names, SSNs and other PII from eBenefits, network information and vulnerability data with VEMS (reference https://www.va.gov/osdbu/docs/news20140218attachment1.docx).

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The VA offices may have initial information to provide to the recipient prior to them signing the form(s)

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

DocuSign does not provide or create any information. Everything is provided by either the VA office sending the request or the recipient.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

DocuSign used as the eSig service if data collected from the services listed in 1.2. This will be collected in the form of uploaded forms by a representative, and a link generated within an email sent to a requested signee. The signee will click the link within the email and will fill out the form with required information and apply their stored signature or create a signature to apply to a document. Once the document is saved from the signee's perspective, the session is completed, and the requestor can download the signed document.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

DocuSign does not utilize the data on the forms. It is responsible for storing the signed form until it is retrieved

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

DocuSign is utilized which is used to verify the information listed in 1.1. Although DocuSign doesn't retain the information, the information is potentially included as a user receives a document for signing.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

DocuSign doesn't check any information for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

This system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304.Identity and Access Management is not a System of Records and the only PII received from the system is data from Master Veterans Index (MVI) which is a System of Record. The MVI System of Record Notice is 24VA10P2 and also System of Records 121VA19 – National Patient Databases-VA. The SORN, 24VA10P2 permits IAM-E correlation of data, to include PII, with the Master Veterans Index (MVI). Additionally, VA internal consuming applications may request specific data from IAM-E services that may include PII. Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397.The SORNs that are relevant are VA SORNs. Those include: 145VA005Q3 (Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA); 146VA005Q3 (Department of Veterans Affairs Identity Management System (VAIDMS)-VA); 150VA19 (Administrative Data Repository-VA); 121VA10 (National Patient Databases-VA); 138VA005Q (Veterans Affairs/Department of

Defense Identity Repository (VADIR)-VA); 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records - VA); 58VA21/22/28 (Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA); (Supplementary Information paragraph b, section 2) dated 7/27/2009 permits the collection of information for the application and verification of military benefits for Veterans. DPR 34 allows the collection of PII for the purposes of establishing human resources records.
https://www.oprm.va.gov/privacy/systems_of_records.aspx eBenefits The legal authority for the eBenefits portal is Title 38 U.S.C. Section 5106. "The head of any Federal department or agency shall provide such information to the Secretary as the Secretary may request for purposes of determining eligibility for or amount of benefits or verifying other information with respect thereto. The cost of providing information to the Secretary under this section shall be borne by the department or agency providing the information "Nationwide Healthcare (NVW)NVW system is to address and comply with Executive Order 13410 "Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs". This Executive Order requires federal agencies to use recognized health interoperability standards to promote the direct exchange of health information between federal agencies and with non-federal entities in supporting quality and efficient health care. The system's legal authority for operating the system, specifically the authority to collect the information listed in Question 1.1 is the Data Use and Reciprocal Support Agreement (DURSA) - an agreement between Health Information Exchange (HIE) partners/organizations and VA information systems. The DURSA provide the legal framework governing participation in the NVW by requiring the signatories to abide by a common set of terms and conditions. These commons terms and conditions support the secure, interoperable exchange of health data between and among numerous NVW partners. Title 38, United States Code, Sections 501(b) and 304. Title 38, United States Code, section 7301(a).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The risk would be the loss of data. The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: This system is intended to be used by authorized VA network users for viewing and retrieving information except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA, the documents are encrypted while stored, and are protected by permissions; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. >>

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

VHA: Uses the following data elements for identifying patient/Veteran for medical purpose: Name, Social Security Number, Date of Birth, Personal mailing address, personal phone number, Drug Allergy, Patient ID and Personal Health information. VBA: Uses the following data elements for identifying patient/ Veteran for Benefit purpose: Name, Social Security Number, Date of Birth, Personal mailing address, personal phone number, Financial Account Information, Certificate/License numbers, Race/Ethnicity, Tax Identification Number. These data elements are mentioned as the document itself could contain the information, thus exposing the documents could cause a risk to privacy. The DocuSign SaaS in no way uses these data elements and is only the VA department requesting the information who will use it for their stated purpose. Name: Identify signer

of the form, Social Security Number: Possibly used as a patient identifier, Date of Birth: Possibly used to identify patient age and confirm patient identity, Mother's Maiden Name: Possibly used for further clarifying the identity of the patient for VA customer, Personal Mailing Address, Personal Phone Number(s), Financial Account Information: Possibly used for payment purposes, Account numbers, Certificate/License numbers, Race/Ethnicity, Tax Identification Number, Drug, Allergy, Patient ID and Patient Health Information: Possibly used for patient identity and medical data for patient records. DocuSign allows customers of the service to upload documents for employees, contractors, and veterans to digitally sign and fill out information on the form. The VA customers of the eSig service use DocuSign to comply with laws such as the Paper Reduction Act, and to save considerable time and effort in getting a document signed by a veteran. DocuSign allows the customers and users to complete signature transactions to support the customers business objectives. The system is uniquely positioned to verify the identity of employee, contractor, veteran and third party and can apply the appropriate permissions to the user's (requestors) session so that the DocuSign services can be utilized without having to set up individual accounts. This reduces the administrative burden for managing the system. Offices in section 1.2 are the current VA offices that utilize the service.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

DocuSign does not use analytic tools on customer data.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

DocuSign does not create or make available any new or previously utilized information.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

To ensure VA data stay protected, DocuSign follows industry best practices to: Logically separate individual customer data; Encrypt customer data – all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing; Support only recognized cipher suites; and Encrypt all documents with AES 256-bit encryption or the most recent FIPS-approved methods.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

To ensure VA data stay protected, DocuSign follows industry best practices to: Logically separate individual customer data; Encrypt customer data – all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing; Support only recognized cipher suites; and Encrypt all documents with AES 256-bit encryption or the most recent FIPS-approved methods. The forms held in the DocuSign platform are flat files with no back-end database to collect this information. The form is stored as a PDF document and once signed by all parties, is not able to be manipulated or deconstructed of information entered on the forms. After 6 months, the documents are no longer accessible, so they need to be downloaded by the proper VA group and stored in a VA-owned document repository. DocuSign personnel are not able to access the documents.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

This system is Fed RAMP Moderate and DocuSign doesn't store any PII/PHI. As authentication for DocuSign is completely reliant upon IAM to establish the connection between the user and DocuSign, the system employs the following measures described in OMB M-06-15 and 16: Implement protections for personally identifiable information being transported and/or stored offsite– This step involves ensuring the proper security controls including encryption are applied to sensitive agency data before it is transported or store away from the main agency network. IAM system data is encrypted in rest and in transmission. Another protection in accordance with OMB is the implementation of protections for remote access to personally identifiable information. All users to IAM systems must have two factor authentication and use RESCUE or Approved VA CAG for entry into the system.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

There is no backend access. Individuals with permissions into the documents are the only ones with access to the appropriate documents which may contain PII. A VA office has the PII information and provides it on a form in DocuSign. The DocuSign forms are blank until a VA office enters information. If a VA office sends a prefilled form, they have the information and DocuSign does not have this information stored.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Users are authenticated through IAM SSO before being authorized to open the documents. All eContracts or eDocuments created by our customers when using the DocuSign eSignature service are automatically encrypted with an AES 256-bit, or equivalent, encryption key. The segmentation and systematic encryption (and key escrow management) employed by DocuSign doesn't allow DocuSign personnel to view or read eDocument content sent through DocuSign eSignature for electronic signature. In accordance with DocuSign's Acceptable use Policy, only select DocuSign personnel (based on role/responsibility) with a demonstrated need to know have access to transactional data surrounding the envelopes.

2.4c Does access require manager approval?

Yes, VA users are authenticated through IAM SSO before being authorized to open the documents. Recipients, asked to fill out and sign VA sent documents via DocuSign are not required to have a VA account, as such, no account is created for recipients.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes. Individuals with permissions and are authenticated are permitted with access to the appropriate documents which may contain PII. Actions are logged/recorded.

2.4e Who is responsible for assuring safeguards for the PII?

To ensure VA data stay protected, DocuSign follows industry best practices to: Logically separate individual customer data; Encrypt customer data – all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing; Support only recognized cipher suites; and Encrypt all documents with AES 256-bit encryption or the most recent FIPS-approved methods. DocuSign utilizes end-to-end TLS to establish secure viewing and signing sessions, document exchange and content, and signature events through the

console from a workstation or mobile device. The VA users who created the documents and download those completed forms are responsible for safeguarding the information on those forms by using a VA Document repository that is secure to the level of the information on that form. As well, VA employees are trained regarding the safeguarding of PII in their mandatory annual TMS 10176 VA Privacy and Information Security Awareness training. DocuSign will alert the VA of any data breaches and has intrusion detection systems which detect and report malicious activity.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

DocuSign is not a system of record only the requesting systems are retaining that information.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

DocuSign is not retaining information. DocuSign is a tool used by the appropriate agency so they can get signatures. Customers using the DocuSign are responsible for the document retention within the appropriate NARA timeframes.
The following are the systems using DocuSign and the length of applicable to the specific system that requested the form to be signed.

- eBenefits' retention policy: No PII or PHI is retained by EBN or VDC only transaction and application form/status information is retained by EBN or VDC for a maximum of six months.

- Nationwide Healthcare's retention policy: NARA guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. Whenever technically feasible, all records

are retained indefinitely in the event of additional follow-up actions on behalf of the individual. However, any documents that the veteran requests removal from the system will be purged from the system upon request.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

DocuSign is not a system of record and only the requesting systems are retaining that information.

3.3b Please indicate each records retention schedule, series, and disposition authority.

DocuSign is not retaining information. DocuSign is a tool used by the appropriate agency so they can get signatures. Customers using the DocuSign are responsible for the document retention within the appropriate NARA timeframes.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

DocuSign is not retaining information. DocuSign is a tool used by the appropriate agency so they can get signatures. The systems using DocuSign will follow electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Handbook 6500 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the

risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

N/A, PII is not used for research, testing or training in DocuSign

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: << Possible risks of data being retained can include data loss, misuse, unauthorized access, and unauthorize disclosure and alteration. >>

Mitigation: << DocuSign uses physical, electronic, and managerial tools. We apply these tools based on the sensitivity of the personal information we collect, use, and store, and the current state of technology. DocuSign protects users' personal information through technical and organizational security measures to minimize risk >>

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Identity and Access Management (eBenefits and Nationwide Healthcare)	To track, and authorize users	Personally Identifiable Information (PII), Individually Identifiable Information (III)	REST/HTTPS

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: <<There is a risk that information could be accessed by unauthorized individuals.>>

Mitigation: << Security controls are in places such as authentication, access and audit logs, use of PIV, and encryption. Users can only access if the information if they've been granted access by their manager.>>

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received /***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN***	***List the method of transmission and the measures in***

	transmitted with the specified program office or IT system		***routine use, etc. that permit external sharing (can be more than one)***	***place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: << Customer data is not shared outside of DocuSign >>

Mitigation: <<N/A>>

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

145VA005Q3 (Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA); 146VA005Q3 (Department of Veterans Affairs Identity Management System (VAIDMS)-VA); 150VA19 (Administrative Data Repository-VA); 121VA10 (National Patient Databases-VA); 138VA005Q (Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA); 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records - VA); 58VA21/22/28 (Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA) For further information on the listed SORNs please visit link: https://www.oprm.va.gov/privacy/systems_of_records.aspx

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

DocuSign Federal -Enterprise SaaS does not provide any notices outside of the published SORNs. Any VA business line using this platform must follow their prescribed notification policy for making the signatory aware of the privacy policies before collecting any information.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

DocuSign Federal -Enterprise SaaS does not provide any notices outside of the published SORNs. Any VA business line using this platform must follow their prescribed notification policy for making the signatory aware of the privacy policies before collecting any information.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes, but no penalty attached. Individuals are only utilizing DocuSign to sign forms. Their information isn't being used for any other purpose. There is no additional information provided by the individual.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

DocuSign is used as a service called eSig. DocuSign is used for individuals to sign forms, and information within it comes from customers of eSig service. They are responsible for receiving applicable consents.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: << Risk that individual is unaware that their information is being collected by the system >>

Mitigation: << DocuSign is only being used for individuals to sign forms. Information is coming from customers eSig service, and they will have their own PIA and notices>>

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be***

listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Information would be attained by veteran names, and other identifiers, so they can request through the Privacy Act Request. Under VHA, veterans can request under HIPPA. Individuals can download the signed documents/forms and reach out to sender for a copy.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

This system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. Individuals are immediately able to access the signed document or reach out to the requesting system for a copy. All other information can be found in DocuSign Federal -Enterprise PIA or requesting system's PIA. If anything needs to be changed in a document/form, user will go to requesting system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If anything needs to be changed in a document/form, user will go to requesting VA department. DocuSign forms are not able to be resent to recipients for corrections, the requesting VA departments will need to start a new request.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The VA department, sending the request document is required to provide the procedures for correcting information. Individuals are immediately able to access the signed document or reach out to the requesting system for a copy. VA standard policy is to request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Redress is provided through VA policy. VA Handbook 6300.4 - PROCEDURES FOR PROCESSING REQUESTS FOR RECORDS SUBJECT TO THE PRIVACY ACT If anything needs to be changed in a document/form, user will go to requesting system.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: << There is a risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information. >>

Mitigation: << Individuals are immediately able to access the signed document or reach out to the requesting system for a copy. If anything needs to be changed in a document/form, user will go to requesting system. >>

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

The VA customer submit a Service Request via an approved intake system. It will go through an internal approval for their specific use case for accuracy. Once approved, they will go to an initial implementation meeting to discuss their need, they will need to provide funding for DocuSign envelopes for their need. Once this is all approved and funded, they will be given access to use the system as a VA Sender. They will only be able to use the specific documents for their use case based on their approved group and access to the group. The segmentation and systematic encryption (and key escrow management) employed by DocuSign doesn't allow DocuSign personnel to view or read eDocument content sent through DocuSign eSignature for electronic signature. In accordance with DocuSign's Acceptable use Policy, only select DocuSign personnel (based on role/responsibility) with a demonstrated need to know have access to transactional data surrounding the envelopes.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

DocuSign's personnel logical access authorization chain requires direct manager approval, application/data source owner approval, and, in cases of sensitive applications and data sources, security management approval. Access to critical applications and data sources is removed at personnel termination and is reviewed to verify that appropriate and current access levels are maintained. DocuSign is ISO 27001 certified and maintains formal policies and procedures for access control. DocuSign enforces the "rule of least privilege" and has documented segregation of duties. We also enforce formal logical and account separation of the development, QA and production environments. On the customer side – access to data is managed by the designated VA site administrator. For a detailed explanation of the available roles, please refer to the guide on permission sets: https://support.docusign.com/en/guides/ndse-admin-guide-permission-sets

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

DocuSign enforces the "rule of least privilege" and has documented segregation of duties. We also enforce formal logical and account separation of the development, QA and production environments. On the customer side – access to data is managed by the designated VA site administrator. For a detailed explanation of the available roles, please refer to the guide on permission sets: https://support.docusign.com/en/guides/ndse-admin-guide-permission-sets.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

No, contractors do not have access to any documents routed through DocuSign.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Privacy Security Awareness Training, and Rules of Behavior Training are required.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* DocuSign Federal -Enterprise
2. *The System Security Plan Status Date:* 6/29/2023
3. *The Authorization Status:* 1-year ATO
4. *The Authorization Date:* 8/22/2023
5. *The Authorization Termination Date:* 8/21/2024
6. *The Risk Review Completion Date:* 7/14/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

This system is FedRAMP Moderate, Software as a Service (SaaS) product.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes, NNG15SD39B 36C10B21F0063

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and

audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

Yes, they provide a monthly usage report. The CSP does not have access to any completed signed forms or any data on those forms. They can only see the usage of the DocuSign envelope.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, this is provided in the contract.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2023.09.14 10:27:02 -05'00'

Privacy Officer, Lynn Olkowski

YENTL BROOKS

Digitally signed by YENTL BROOKS
Date: 2023.09.11 14:31:38 -05'00'

Information System Security Officer, Yentl Brooks

April D. Primous 1632179

Digitally signed by April D. Primous 1632179
Date: 2023.09.13 14:05:12 -05'00'

Information System Owner, April Primous

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

For further information on the listed SORNs please visit link:
https://www.oprm.va.gov/privacy/systems_of_records.aspx

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices