Privacy Impact Assessment for the VA IT System called:

Adobe Acrobat Sign for Government -E

Veterans Health Administration

Albany Stratton VA Medical Center (VAMC)

eMASS ID 2564

Date PIA submitted for review:

08/29/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christopher Ashe	christopher.ashe@va.gov	518-626-6944.
Information System Security Officer (ISSO)	Martin DeLeo	martin.deleo@va.gov	202-699-6495
Information System Owner	Scottie Ross	scottie.ross@va.gov	478-595-1349

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Adobe Acrobat Sign for Government -e is a cloud-based software as a service allows for documents to be accessed and signed by multiple parties in a dynamic manner while maintaining a static single document. This SaaS will allow the Department of Surgery to manage multiple streams of communications and document flow in a more efficient and effective manner, with anticipated significant impact on quality and patient safety. By way of maintaining a single document in the cloud, we avoid having the document disseminated by email, and having multiple documents with fragmented signature streams needing to be consolidated with multipage and multifile records.

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. What is the IT system name and the name of the program office that owns the IT system?

Adobe Acrobat Sign for Government -e will be owned by the SaaS Vendor but controlled by the Albany Stratton VA Medical Center.

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

This SaaS provides a way of maintaining a single document in the cloud, avoiding disseminating charts for signature by email, and having multiple documents with fragmented signature streams needing to be consolidated with multipage and multifile records.

C. Who is the owner or control of the IT system or project?

The system is VA Controlled / non-VA Owned and Operated.

2. Information Collection and Sharing

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

There are at the minimum three parties involved in Signing Workflow:

- Individual Sending an Agreement – This number of individuals is equal to the number of Users that VA will provision on Adobe Acrobat Sign.
- Individual Signing an Agreement – Number of individuals is variable and is dependent on who the agreement is sent to.
- Patient and their information pertaining to chart reviews.

Total expected number of users – 2000.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The system will collect identifying information to validate the chart patient and the signatory and their permissions. This is collected to allow for signature of charts.

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

Information sharing conducted by the system is limited to Full Name, Position, Title, Fee Basis Providers, Demographic, Education, Training, Licensure, Certifications, FPPE/OPPE, and Contact information. All information sharing to and from the system is for the purpose of form and document creation for signature and signature requests. This information is manually entered into the Adobe Acrobat Sign for Government system by the creator if any form or document in the Albany Stratton VAMC Department of Surgery.

G. Is 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?

This is a cloud-hosted system, which is operated from one site with 3 availability zones.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

Health Insurance Portability and Accountability Act of 1996 (HIPAA), VA Directive 6500 Managing Information Security Risk: VA Information Security Program.

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?

Per the PTA a SORN is not required for Adobe Acrobat Sign.

4. System Changes

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

Yes. The document processing workflow will be adapted to the Adobe Sign System

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

Yes, would allow exchange of documents to flow in a closed, more secure system.

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☐ 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)

Other PII/PHI data elements: Position, Title, Professional/VA/Academic email, Office phone number, Last 4 of SSN, Demographic, Education, Training, FPPE(Focused Professional Practice Evaluation) /OPPE (Ongoing Professional Practice Evaluation), Certificate/License numbers (State licenses, DEA registrations, board certifications)

PII Mapping of Components (Servers/Database)

Adobe Acrobat Sign for Government consists of **1** key component (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Adobe Acrobat Sign for Government** and the reasons for the collection of the PII are in the table below.

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
VISTA/CPRS	Yes	Yes	last name initial, last 4 of patient SSN	Chart/patient identification and connection	Data is Encrypted in transit (TLS 1.2) and at rest (AES 256)

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?

Patient information is collected from patient at time of provision of care. VA employee, contractor, and other care provider information is collected from clinicians, doctors, and other care providers at time of hiring or engagement of work.

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.

Patient information is pulled from VISTA/CPRS as that is where the information is stored after the time of initial care provision.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

System creates an Audit Trail of the Signing Process. Users Provisioned into the system can run and generate reports.

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?

Information is either solicited directly from the custodian of that information (i.e. HR< credentialing/privileging services etc.) or through the transmission of electronic files from various sources. No integration with other services/databases.

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

VA Form 7468 is used to destroy records at this facility.

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.

Information is checked manually by parties associated with the documents. The information is manually checked at least once on intake, once when Service Chief signs a document, and once by receiver of document.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system does not check 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

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers the collection of patient information at the time of care.

- VHA Directive 1605.01 Privacy & Release of Information covers collections of all end user information and the sharing of information necessary for the completion of forms and documents needing signature.

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: Transmission of PII over enterprise email exposes that data to risk of inappropriate access.

Mitigation: Currently manage through encrypted email, targeted flow of info to email addresses. Adobe sign will cut down number of handoffs. Encryption on VA sensitive information has been in place internally. Use of Adobe sign would reduce the number of handoffs through current practice of emailing documents between associated parties.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Patient Last Name Initial	File Identification purposes	Not used
Last 4 of patient SSN	File Identification purposes	Not used
Full Name	Provider and signatory rights verification	Provider and signatory rights verification
Position	Provider and signatory rights verification	Provider and signatory rights verification
Title	Provider and signatory rights verification	Provider and signatory rights verification
Demographics	Provider and signatory rights verification	Provider and signatory rights verification
Education	Provider and signatory rights verification	Provider and signatory rights verification
Training	Provider and signatory rights verification	Provider and signatory rights verification
Certifications/Licensure	Provider and signatory rights verification	Provider and signatory rights verification
FPPE/OPPE	Provider and signatory rights verification	Provider and signatory rights verification
Contact Information (personal/professional/academic/VA email, office phone number, personal phone number)	Provider and signatory rights verification	Provider and signatory rights verification

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?

The System does not analyze data. System has reporting capability that provisioned users have access to and can generate reports.

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.

The System does not analyze data. System has reporting capability that provisioned users have access to and can generate reports.

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?

AES 256-bit encryption at rest; HTTPS TLS v1.2 or higher in transit.

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

System doesn't collect SSN but can be collected as part of filling out agreements forms that require SSN. SSN information collected via Agreement Form input is encrypted at rest using AES 256. The captured SSN can be masked when submitted Form is viewed.

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

The system complies with FedRAMP Moderate control requirements and safeguard customer data in accordance with those requirements. The following controls from NIST Special Publication 800-53 are in place to address standards and guidelines for federal information systems:

- AT-1: Security and Awareness and Training
- AU-7: Audit Reduction and Report Generation
- AU-9(4): Protection of Audit Information / Cryptographic Protection
- PS-3(3): Personnel Screening -Supplemental Screening
- SC-28: Protection of Information at Rest

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

Access to PHI is determined by role and at the discretion of the Service Chief.

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

Documented through form 10-0539 – Assignment of Functional Categories.

2.4c Does access require manager approval?

Yes

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

Yes, personnel are tracked in the individual systems being accessed.

2.4e Who is responsible for assuring safeguards for the PII?
Local Privacy Team for facility.

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*

By default, the system retains in flight and completed Agreements and associated filled form data and attached documents and Audit Report. Please see this page https://helpx.adobe.com/sign/using/manage/activity-log.html. System offers the flexibility to automatically purge aged Agreement data. The following information is collected and retained: First Name, Last Name, Email Address.

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.

Records should be maintained and/or disposed of in accordance with Records Control Schedule 10-1, Item Number 1001.2 Non-recordkeeping Copies of Electronic Records. All forms and documents sent via the system are working documents. The correspondence in the system will be destroyed immediately once the final document is completed. The completed document will go to the appropriate service and that service will store the document until expiration.
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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?

Yes.

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

Records should be maintained and/or disposed of in accordance with Records Control Schedule 10-1, Item Number 1001.2 Non-recordkeeping Copies of Electronic Records, Disposition Authority GRS 5.1, item 020, DAA-GRS-2016-0016-0002.
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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.

By default, the system securely retains all customer documents on the service for as long as the account is active. Transactional information persists in the system until the customer takes action to delete the agreements explicitly. For customers that prefer to store their agreement records in their own systems and want to delete the original documents from the Acrobat Sign systems, a "retention policy" can be defined that asserts how long the system should retain the transaction, and automatically delete the agreement (and optionally the supporting audit/personal data) from the system after that timespan. Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is

wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1.

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.

No Customer information is used for research/testing/training.

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: The system requires and retains Name and Email Address, which are identifiable and at risk if accessed inappropriately.

Mitigation: The system encrypts this information in motion and at rest and can be eliminated from the system in accordance with VA retention policies or at VA's will.

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***
Department of Surgery	File Identification purposes	last name initial, last 4 of patient SSN	S/MIME Encrypted Email, Adobe Acrobat Sign

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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: The system collects and shares PII, which could pose a privacy risk for the individual if accessed inappropriately or not appropriately protected in sharing.

Mitigation: The system has in place FedRAMP Moderate controls (~325+ controls) to protect customer information. Customer information is always encrypted in motion and at rest.

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	***List the purpose of information being shared / received / transmitted with the***	***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 routine use, etc. that permit external sharing***	***List the method of transmission and the measures in place to secure data***

shared/received with	***specified program office or IT system***		***(can be more than one)***	
Adobe Acrobat	File Identification and signature purposes	Full Name, Position, Title, Fee Basis Providers, Demographic, Education, Training, Licensure, Certifications, FPPE/OPPE, Contact information	NASA SEWP Contract NNG15SD38B	AES 256-bit encryption at rest; HTTPS TLS v1.2 or higher in transit

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: PII is shared to the system, which is external to VA. This could pose a privacy risk for the individual if accessed inappropriately or not appropriately protected in sharing.

Mitigation: The system has in place FedRAMP Moderate controls (~325+ controls) to protect customer information. Customer information is always encrypted in motion and at rest.

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.

This Privacy Impact Assessment (PIA) serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

This PIA serves as notice.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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.

Notice is adequate as indicated in 6.1a
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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.

Previously given information to be pulled from existing systems to complete forms. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. Any information not provided, or forms not electronically signed could lead to a suspension in the processing of the form and any actions consequent to the forms.

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.

Employees, contractors, Veterans, and beneficiaries are required to provide information and consent to use of information, including and not limited to the intent and purpose of the form, for processing of the form, and any subsequent/consequent processes.

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: There is a risk that an individual may not understand why their information is being collected or maintained about them.

Mitigation: This risk is mitigated by requiring employees and contractors to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness. Risk is mitigated for veterans and beneficiaries by HIPAA agreements at the time of care, and further mitigated by provision of public notice via the PIA.

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.***

- VA Freedom of Information Act
- HIPAA
- 5 CFR Part 294
- Specific end users may inquire about submitted information, in part or in whole, and be provided a response at the discretion of the service in accordance with HIPAA, FOIA, and other VA privacy requirements external to the Adobe Sign service.
- When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at https://www.va.gov/find-forms/about-form-10-5345a/. Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the my HealtheVet program, VA's online personal health record. More information about my HealtheVet is available at Home - My HealtheVet - My HealtheVet (va.gov)

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)?

The system is not exempt from 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?

The system is a Privacy Act 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.

A Form with incorrect information can be cancelled and a new Form with correct information can be triggered by VA. Service line responsible for the information provided will be responsible to correct information. Any request for information corrections would need to be triggered by the subject of the information. VA would identify the owner of the information and correct internal to the Adobe Sign system or direct to appropriate service line for further action.

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.

Service maintains standard practice where all end users are able to communicate to administrative staff for any queries relating to accurate information. Notice may be verbal or written.

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.

Formal redress is provided as outlined above in 7.3 and 7.4. End-users may contact the administrative staff of the service line that owns the information to correct it accordingly. The respective form in the Adobe acrobat Sign for Government system would then be able to be appropriately corrected.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, in creation of forms and providing opportunity for end users to request correction through administrative staff.

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?

Internal VA Users and admin must be explicitly added by an existing Admin. VA can also require internal users to be authenticated with their Active Directory. External participants are typically notified via email that there is a document that requires their attention. These participants must be added to a Sign workflow by an internal user and can be verified by a number of different identity authentication options including email, password, id.me, login.gov and more. This is all documented on the Acrobat Sign support site: https://helpx.adobe.com/contact.html.

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?

It is possible that other agencies would have access to system as signers only. PII would only be shared with VA-affiliated personnel as verified VAMC administrative staff.

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.

The system service provides a multi-level authority system to provide access and tools to identified users. Users can hold one or more levels of authority.

The current levels of authority can be summed up as:

- **Signers** - Signers have authority specific to the agreements they have been sent. They can view, decline or complete an agreement. Their Manage tab retains the history of the agreements sent to them, and they have the authority to view and print these agreements.
- **Senders** - Senders are registered users that have full access to the Acrobat Sign interface. Authority within the terms of an agreement includes the ability to send an agreement, replace or modify an agreement they have sent, reporting against their agreements and templates. Additional tools include the event notification system, reminders, account sharing, language/locale configuration, and other tools specifically designed to improve the personalization of the sender's account.
- **Group Admins** - Group Admins have the authority to override the account-level settings and configure the group they are in to better reflect the work product of the

group. This includes most account-level settings, including branding, default signature and verification settings, workflows, templates, etc.

- **Account Admins** - Account admins control the settings at the account level. Account-level settings are automatically inherited by all groups in the account unless the group-level admin overrides them (see above). At the account level, admins can configure settings like federated sign-in, Account level branding, templates, and workflows.
- **Privacy Admins** - The Privacy Admin is an extension of the Account admin role. Privacy admins must first be an Account admin to add the additional toolset. The privacy admin has the authority to fully delete agreements and userIDs from the Acrobat Sign servers (per GDPR requirements).

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.

Contractors would only have access as end-users and/or signers. VA Contractors must review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training.

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 Training is provided to Adobe users as part of Adobe's Awareness Training. All VA users must review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training and the Privacy and HIPAA Training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>

2. *The System Security Plan Status Date:* <<ADD ANWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date: <<ADD ANSWER HERE>>*
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

The system is In Process of VA's A&A process through the Digital Transformation Center. The system is already FedRAMP authorized at a Moderate Impact Level. The IOC within VA is estimated for 01/15/2025 but could be earlier.

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 a Software as a Service (SaaS) that uses cloud technology with hosting in Azure US East. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR2108360349.

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.*

Contract No: NNG15SD38B, Order # 36C24224F0165, local contracting purchase order 528C43148.

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.

The system only requires Name and Email address. Any additional data collected is at the discretion of the organization administering the system and will remain in the ownership of the administering organization. In this case, that organization is VA.

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.

At the time of submission, updated SaaS language was not available. Language to be added next available opportunity to modify statement of work. Agency still intends to operate system in accordance with NIST 800-144.

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).

This system does not utilize RPA.

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

CHRISTOPHER ASHE

Digitally signed by CHRISTOPHER ASHE
Date: 2024.09.12 08:16:39 -04'00'

Privacy Officer, Christopher Ashe

JOHN DELEO

Digitally signed by JOHN DELEO
Date: 2024.09.12 08:27:57 -04'00'

Information Systems Security Officer, Martin DeLeo

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2024.09.12 08:36:56 -04'00'

Information Systems Owner, Scottie Ross

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; screen shot of a website collection privacy notice).

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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