Privacy Impact Assessment for the VA IT System called:

Box Enterprise Cloud Content Collaboration Platform-E

Office of Information and Technology

Project Special Forces VACO

eMASS ID #1170

Date PIA submitted for review:

4/04/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov oitprivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Anna Johnson	Anna.Johnson3@va.gov	520-629-4930
Information System Owner	Herbert Ackermann	Herbert.Ackermann@va.gov	202-461-0543

Abstract

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

Box is an enterprise content management platform that solves simple and complex challenges, from sharing and accessing files to sophisticated business processes like data governance and retention. The Box enterprise content management platform enables business to easily store, share, manage and secure their content (documents, data, files, and videos). In today's cloud-first world, providing employees with secure access to content at any time using any device is critical to creating a more productive, connected workforce and improved customer experiences. Beyond secure file sharing, Box enables easy access to content and collaboration. In addition to Box's core content management platform offering, customers have more control over their content to meet security, compliance, and privacy requirements.

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?*

The IT system name is Box Enterprise Cloud Content Collaboration Platform-E and it is owned by Project Special Forces- VACO.

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

Box is a cloud-based, ready-to-use software empowers team members to communicate and collaborate securely. To protect the team's sensitive information, Box utilizes intelligent threat protection, advanced security controls, and complete information governance. Box provides a secure method for VA a non-VA affiliates to share, store, and receive information.

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?*

The expected number of individuals whose data will be stored within the system is 800 (internal and external users). The typical clients are business owners and researchers who need to a secure tool to send documents and collaborate.

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

The information within the IT system may be PII such as name, email address, phone number, SSN, and PHI like medical records and prescriptions. The purpose of collecting this information is solely for addressing business owners need for a secure tool that can collect sensitive data for research.

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

There are 2 components to the system which are Switch, Nevada-Primary and Vantage, California Alternate Data Center.

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?*

The system is hosted on a commercial cloud. Google Cloud Platform is the Cloud Service Provider (CSP).

3. Legal Authority and SORN

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

121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023 https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf (Legal Authority: 38 U.S.C 501)

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.federalregister.gov/documents/2022/07/01/2022-14118/privacy-act-of-1974-system-of-records
(Legal Authority: 42 U.S.C. 2165)

150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf
(Legal Authority: 38 U.S.C. 1)

172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
(Legal Authority: 5 U.S.C 552)

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?*

No update to SORNs required.

4. System Changes

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

There are no major system changes to report.

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

The completion of this PIA will not result in any technology changes.

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: SECID (Investment company Identification Number), VA Program Business Owner Assigned Number (routinely used), VA email address

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

PII Mapping of Components (Servers/Database)

Box consists of **2** key components (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 **Box** 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 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**
Switch, Nevada – Primary	Yes	Yes	Name/ SEC ID	Registration	Stored encrypted, subject to very strict guidelines compliant to our various government certifications like FedRAMP Moderate
Vantage, California – Alternate Data Center	Yes	Yes	Name/SEC ID	Registration	Stored encrypted, subject to very strict guidelines compliant to our various government certifications like FedRAMP Moderate

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 data comes directly from the invividuals. Some of the information may be research based and contain both PII/PHI The information obtained from Box is not using commercial aggregators or analysis.

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.*

Information from other sources other than an individual is not required for Box.

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

Box does have the ability to generate a report.

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?

The information is collected from individuals.

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?

The information is collected from individuals. The information is not collected on a form.

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.

Customers can check the integrity of a file using hashes. Please see https://developer.box.com/reference#files for more details on checking the hash for the upload. To perform this check, you will need to utilize Box API to make the call for the file's hash (Sha1). Admin will verify the information is correct before individual can receive credentials to use Box.

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 use a commercial aggregator to check information for accuracy.

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

121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf (Legal Authority: 38 U.S.C 501)

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.federalregister.gov/documents/2022/07/01/2022-14118/privacy-act-of-1974-system-of-records
(Legal Authority: 42 U.S.C. 2165)

150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf
(Legal Authority: 38 U.S.C. 1)

172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
(Legal Authority: 5 U.S.C 552)

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: There is a risk that the information collected in the system is not accurate.

Mitigation: Data is collected from the individual; the individuals have opportunity to correct their information. It is the responsibility of the user to determine if data is accurate. They have the ability to remove data from Box if they believe it is not accurate, since the user is responsible for uploading data into Box.

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
Name	used to appropriate accounts for use, and as an identifier.	May be used/collected to verify entity trying to access information
VA email	used to appropriate accounts for use, and as an identifier.	May be used/collected to verify entity trying to access information
Social Security Number	used to identify the hearing recording for purposes on transcription and ensuring accuracy. The last four digits may show in payroll records. SSN may also be collected for quality improvement projects where Electronic Health Record reviews are required to facilitate and monitor quality improvement efforts.	May be included on the documents shared to authorized viewers externally.
Date of Birth	May be included on documents stored within Box	May be included in documents shared externally
Personal Mailing Address	May be included documents stored within Box	May be included in documents shared externally
Personal Phone Number(s)	May be included documents stored within Box	May be included in documents shared externally
Personal Fax Number	May be included documents stored within Box	May be included in documents shared externally
Personal Email Address	May be included documents stored within Box	May be included in documents shared externally
Financial Account Information	May be included in some of the financial documents stored within Box	May be included in documents shared externally

Health Insurance Beneficiary Numbers	May be included documents stored within Box	May be included in documents shared externally
Certificate/License numbers	May be included documents stored within Box	May be included in documents shared externally
Current Medications	May be included documents stored within Box	May be included in documents shared externally
Medical Records	May be included documents stored within Box	May be included in documents shared externally
Medical Record Number	May be included documents stored within Box	May be included in documents shared externally
VA Program Business Owner Assigned Number (routinely used),	May be included documents stored within Box	May be included in documents shared externally
SECID *(Investment company Identification Number)*	Will be used in Box for verification	May be included in documents shared externally
VA email address	May be included documents stored within Box	Will be included in documents shared externally

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?

Box does not use any tools to analyze 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.

The system does have record retention. With new information a new record is created, but the information is only accessible to individuals who have obtained a license and been provisioned at root level to have access to that folder.

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?

The data is protected by encryption at rest and in transit.

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

The data stored at rest and in transit within Box is protected by end to end 256 Advanced Encryption Standard bit encryption.

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

Box is compliant with the OMB Memorandum. Box does allow for sharing and collaboration with documents that contain PII or PHI with an external 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?

The access to PII is determined by the SSOi and SSOe verification. Each individual would need to verify their identity through PIV card or ID.ME (2 step verification) before they can access their Box account. Box has a moderate ATO, which allows for both PII and PHI.

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

Yes, there are several SOPs, criteria, controls, and responsibilities are being documented and stored within Box.

2.4c Does access require manager approval?

Yes, manager approval is required

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

Box system allows for PHI and PII and logins are tracked/monitored regularly.

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

Information System Owner

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*

The PII/PHI stored within Box are listed below:

- *First and Last name*
- *Sec ID (Investment company Identification Number)*
- *SSN*
- *DOB*
- *Personal mailing address*
- *Personal Fax Number*
- *Gender*
- VA Program Business Owner Assigned Number (routinely used)
- *Financial Records*
- *Personal phone number*
- *Personal email address*
- *Health insurance beneficiary numbers*
- *Certificate/license numbers*
- *Medical Record Number*
- *Internet Protocol Address Numbers*
- *Medical Records*
- *Current medications*
- *Race/ethnicity*
- *Integration Control Number*
- *Next of Kin*
- VA 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.*

The information is retained for 7 years for historical reference and then removed.

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?

The retention scheduled has been approved by the VA. Yes, all records that are stored within the system are approved on disposition authority. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records). 1100.40 Records related to the establishment, development, execution and completion of educational projects, programs and activities of pertinent and accepted modalities for clinicians and non-clinicians working within the VHA health care system. Content areas emphasize broad strategic issues of interest nationally or regionally. a. Paper files. Hardcopy version of information manually entered project/program files. Temporary. Destroy 7 years after the education activity is closed. If an accepted digital copy has been made, destroy immediately. N1-015-11-4, item 1 b. electronic files. Electronic and/or digital version of information entered project/program files. Temporary. Destroy 7 years after the education activity is closed. N1-015-11-4, item 2 c. Media files. A file residing digitally or embedded on tape medium that contains one or more video or audio tracks of data that contain content/essence. Temporary. Destroy 7 years after the education activity is closed. N1-015-11-4, item 3 d. Historically significant media files. Any media file that has significant or lasting value to the Agency and/or the Federal government. PERMANENT. Transfer to NARA 7 years after the education activity is closed. Transfer according to NARA standards in place at the time of transfer. N1-015-11-4, item 4 e. Consent forms (VA Form 3203). Consent for use of picture, video, or voice recording for authorized purposes. Temporary. Destroy 60 years after project is closed. If an accepted digital copy has been made, then destroy immediately.VBA-VB-1 RCS, VHA RCS-10-1, and OIT RCS 005-1 are applicable retention schedules that apply to VA Box.

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

The following record retention schedule, series, and disposition authority are applicable for Box: N1-015-11-4 item 1b electronic files; N1-015-11-4, item 2c.Media Files; N1-015-11-4 d. Historically significant media files; N1-015-11-4 ITEM 4 E. Consent forms (VA forms 3203); VBA-VB-1 RCS; VHA RCS-01-1, and OIT RCS 005-1.

Box Admins can generate report on the creation, editing, and retiring of a policy (administrative actions). Admins can also report on the application of policy to files as part of an end-of-policy Disposition Action. The default retention policy for Box use within the VA is 7 years. When retention policies are configured with an end of policy Disposition Action, content is queued for deletion after its applicable retention period expires. While files identified for deletion are often deleted the same day the retention period ends, disposition timeframes may vary and cannot be guaranteed. Additionally, for enterprises with extremely large volumes of content, delays in disposition may occur in some cases. Lastly, Box Governance's disposition identification process can affect disposition timing in the following rare scenarios:

Scenario:
As part of a customer sandbox experiment, you apply a retention policy of one day to a file
Result:
The disposition identification process is run on customer sandboxes daily, so the file is now eligible for deletion after one day elapses.

Scenario:
Given a file that is under an Event-Based Retention (EBR) policy of three years, you set the retention start date to exactly three years ago.
Result:
The disposition status will be recognized in the next disposition identification process. and the file will be eligible for immediate deletion when the process runs.

Scenario:
Given a file that was uploaded to Box five years ago, you apply a retention policy of three years to the file's parent folder.
Result:
The disposition status will be recognized in the next disposition identification process. and the file will be eligible for immediate deletion when the process runs.

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.

Users can delete retained files by sending them to Trash. However, users cannot purge files from Trash until the files' retention period has ended. Before that time, users can also restore files from Trash to their original location. If the original location has been deleted, users can choose a new folder in which to restore the files.

When a file is governed by a retention policy, an indicator displays under the Details section in the righthand navigation. You also see this information by clicking the More options arrow to the right of the file name and then selecting Properties > General Info.

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.*

The system does allow for storage of PII and PHI for research and other use cases. Due to the increase of risk associated with storing data, Box has maintained an ATO to store data at high impact. Box does not directly use PII for testing new applications or information systems prior to deployment. Box serves as secure repository for data that has both PII and PHI.

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. The system itself does use techniques to help minimize the risk. Box has a large amount of customer uses the tool for research purposes. Box is currently using end-to end encryption.

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: There is a risk that data may be stored after project or work is completed. The data may be sensitive and need to be removed at the end of project.

Mitigation: Box has a retention policy in place. The data will be stored within Box securely and protected by 256-bit end to end encryption. After 7 years, the data will be manually deleted from Box. Depending on use case or project, the data can also be removed as soon as the project ends.

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***
VA Employees	This data will be used to highlight highly sensitive information pertaining to investigations within the VA. Will contain both PII and PHI. Will include information related to the criminal investigation process	• First and Last name • Sec ID (Investment company Identification Number) • SSN • DOB • Personal mailing address • Personal Fax Number • Gender • VA assigned number • Financial Records • Personal phone number	Data entered by VA employee. VA Employee receives data via various methods. Box uses (FTP) File Transfer Protocol for migration and transfer of content. FTPS

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*
		• Personal email address • Health insurance beneficiary numbers • Certificate/license numbers • Medical Record Number • Internet Protocol Address Numbers • Medical Records • Current medications • Race/ethnicity • Integration Control Number • Next of Kin	is also supported. TLS 1.3 is used to encrypt content uploaded to Box in transit
Box.com	Transmission of video/audio files of investigative interviews to transcription services (contractors) the contractors are external and do not have VA network access.	• First and Last Name • Email Address	VA employees verify their identity through SSOi (PIV card) or through their va email address and password. VA employees upload data by going to Box.com website in which they have authorized permissions.

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: There is always an inherent risk that data stored within Box can be intentionally leaked (human error).

Mitigation: To mitigate this issue, Box only allows access to users that have a use case for us to place them in the high environment. This environment is restrictive to select programs (listed in chart above). System admins routinely to run user activity/ monitoring reports that show account logins and actions.

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 / transmitted with the specified program office or IT system***	***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 (can***	***List the method of transmission and the measures in place to secure data***

			be more than one)	
Veterans and Dependents	To securely allow data exchange between VA and VA affiliates	• First and Last name • Sec ID (Investment company Identification Number) • SSN • DOB • Personal mailing address • Personal Fax Number • Gender • VA assigned number • Financial Records • Personal phone number • Personal email address • Health insurance beneficiary numbers • Certificate/license numbers • Medical Record Number • Internet Protocol Address Numbers • Medical Records • Current medications • Race/ethnicity • Integration Control Number • Next of Kin	121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023 145VA005Q3 -Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022) 146VA005Q3 -Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) 150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023 172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021	Direct system access. Box uses (FTP) File Transfer Protocol for migration and transfer of content. FTPS is also supported. TLS 1.3 is used to encrypt content User Agreement (Acceptable Use Policy) required for all box account holders.
VA contractors	VA Contractor can upload data into Box environment (once they have	• First and Last name • Sec ID (Investment company Identification Number) • SSN • DOB	121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023	Direct system access. Box uses (FTP) File Transfer Protocol for

	received a license/account	• Personal mailing address • Personal Fax Number • Gender • VA assigned number • Financial Records • Personal phone number • Personal email address • Health insurance beneficiary numbers • Certificate/license numbers • Medical Record Number • Internet Protocol Address Numbers • Medical Records • Current medications • Race/ethnicity • Integration Control Number • Next of Kin	145VA005Q3 -Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022) 146VA005Q3 -Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) 150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023 172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021	migration and transfer of content. FTPS is also supported. TLS 1.3 is used to encrypt content User Agreement (Acceptable Use Policy) required for all box account holders.
Clinical Trainees	Clinical Trainees can upload data into Box environment (once they have received a license/account) . Box uses (FTP) File Transfer Protocol for migration and transfer of	• First and Last name • Sec ID (Investment company Identification Number) • SSN • DOB • Personal mailing address • Personal Fax Number • Gender • VA assigned number • Financial Records • Personal phone number • Personal email address	121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023 145VA005Q3 -Department of Veterans Affairs Personnel Security File System	Direct system access. Box uses (FTP) File Transfer Protocol for migration and transfer of content. FTPS is also supported. TLS 1.3 is used to encrypt

	content. FTPS is also supported. TLS 1.3 is used to encrypt content	• Health insurance beneficiary numbers • Certificate/license numbers • Medical Record Number • Internet Protocol Address Numbers • Medical Records • Current medications • Race/ethnicity • Integration Control Number • Next of Kin	(VAPSFS) (7/1/2022) 146VA005Q3 -Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) 150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023 172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021	content User Agreement (Acceptable Use Policy) required for all box account holders.
Box.com	Box will use full name and email address to verify users attempting to obtain/view data stored within Box.	• First and Last Name • Email Address	121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023 145VA005Q3 -Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022) 146VA005Q3 -Department of Veterans Affairs Identity Management	Direct system access. Box uses (FTP) File Transfer Protocol for migration and transfer of content. FTPS is also supported. TLS 1.3 is used to encrypt content User Agreement (Acceptable Use Policy) required for all box

			System (VAIDMS)-VA (3/26/2008) 150VA10 / 88 FR 75387 Enterprise Identity and System (VAIDMS)-VA (3/26/2008) 150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023 172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021	account holders.

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> There is inherent risk with sharing information. There is a possibly of data being shared to wrong individual due to human error.

Mitigation: Box has encryption method, SSOi, and id.me verification set in place to confirm that only users that have been vetted has access to information/data.

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.

Yes, notice was provided to an individual prior to collection of the information. I have attached the privacy policy for Box here. https://www.box.com/legal/privacypolicy.

Please see below for applicable SORNs:

121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf (Legal Authority: 38 U.S.C 501)

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.federalregister.gov/documents/2022/07/01/2022-14118/privacy-act-of-1974-system-of-records
(Legal Authority: 42 U.S.C. 2165)

150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf
(Legal Authority: 38 U.S.C. 1)

172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
(Legal Authority: 5 U.S.C 552)

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

Notice is provided upon usage of Box.

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.

The notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy

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. The individual would have to submit a written document to Box Privacy team to provide consent to uses of the information. Please see the privacy page for information below. https://www.box.com/legal/privacypolicy.

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.

Yes, the individual does have the right to consent to certain uses of information. Please see the privacy page for information below. https://www.box.com/legal/privacypolicy

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.

<u>Mitigation:</u> Box is only being used as a storage repository of data collected from the individual. When users sign up for Box, they understand that the system itself is a repository of data. The Acceptable Use Policy that every user signs mentions what Box, and that the terms must be agreed to before an account can be provisioned. The data within Box is end to end encrypted by leading 256-bit encryption.

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.***

The Box user uploads their own documents. If users have access to Box, they will have access to any content that they have uploaded to Box.
Procedures to access individually identifiable information are addressed in the Box Privacy Policy under the Personal Information Choices section:
Users can update, access, and delete account information and exercise data protection and privacy rights at any time by logging into their Box account or they can contact Box at privacy@box.com

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 allows for individuals to access their Box User account at any time. The system is not exempt from 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?

This system stores information collected from individuals. Individuals have a Box user account and upload their own documents. Users can update, delete account information, and exercise data protection and privacy rights at any time by logging into their Box account and updating their preferences or by contacting Box at privacy@box.com.

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.

Box users provide their own data/information via account creation and documentation upload. The Box privacy policy does provide a process for users to update, delete account information. Users can log into their Box account and update their preferences or can contact privacy@box.com

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.

Box users control their Box account and documents that are uploaded to their file. Box users can update, delete account information, and exercise data protection and privacy rights at any time by logging into their Box account or by contacting privacy@box.com. The Box privacy notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy

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.

Box users control the information they store within their account. The user can directly access their account to correct/update their information at any time by logging into their Box account or by contacting privacy@box.com. The Box privacy notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy.

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 Privacy Risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

Mitigation: This risk is partially mitigated by the Box user being in control of the information that is uploaded to the account. Individuals can reach out to the local admin for correction purposes. Users may also go to Box's support link for assistance 24/7 to correct information. https://support.box.com/hc/en-us.

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?

To receive access to Box, an individual would need to submit a request with the VA SaaS Catalog, complete a discovery call and obtained a signed DSC/MOU. Once this step is completed, a user will need to fill out a 2237 and ARM memo to purchase a license. Once the license has been purchased, the user must provide pre-provisioning info such as business line and group approver and sign the acceptable use policy form. After the provisioning documents have been completed, a Box admin is able to correctly provision the user to Box and activate the license.

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?

The users from other agencies (VA and Non-VA) will be contractors, researchers, clinical trainees, and other business owners. With guidance from the VA, Box establishes the criteria for what PII can be shared. Individuals who obtain a VA Box license are then able to control what documents that are stored within Box and what information is shared.

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 roles are Editor, Viewer Uploader, Previewer Uploader, Viewer, Previewer, Uploader, Co-owner.
The permission sets described below are utilized as part of the waterfall security design. Permissions are assigned at the top and flow to folders and content down the hierarchy. Admins essentially have the top-level access of co-owners and can control the level of access other have within their group.

Please reference this provided chart as well as this link for a more in depth look at the different permission levels.

- **Co-owner –** A Co-owner has all functional read/write access that an editor does. This permission level has the added ability of being able to change some advanced folder settings. Co-owners cannot change the owner of a folder.

- **Editor –** An editor has full read/write access to a folder or file. Once invited to a folder or file, the editor can view, download, upload, edit, delete, copy, move, rename, generate, and edit shared links, make comments, assign tasks, create tags, and invite/remove collaborators. The editor is not able to copy, delete, or move root level folders.

- **Viewer Uploader –** This access level is a combination of Viewer and Uploader. A viewer uploader has full read access to a folder and limited write access. They can preview, download, add comments, generate shared links, and upload content to the folder. They are not able to add tags, invite new collaborators, or delete items in the folder. To update a file, people with this permission had to download a file, edit it locally, and re-upload (using the same file name). Effective May 2014, these collaborators can use Box Edit to perform the same action (download, edit, and re-upload) seamlessly.

- **Previewer Uploader –** This access level is a combination of Previewer and Uploader. A previewer uploader has limited read and write access to a folder. They can preview, add comments, add tasks, and upload content to the folder. They are not able to add tags, generate shared links, invite new collaborators, edit, or delete items in the folder.

- **Viewer** – A viewer has read access to a folder or file. Once invited to a folder, the viewer can preview, download, make comments, and generate shared links. The viewer is not able to add tags, invite new collaborators, edit shared links, upload, edit files, or delete items in the folder.

- **Previewer** – A previewer has limited read access. The previewer is able only to preview the items in the folder using the integrated content viewer. The previewer is not able to share, upload, edit, or delete any content.

- **Uploader** – An uploader has limited write access. The uploader is able only to upload and see the names of the items in a folder. The uploader is not able to download or view content.

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.

All Box System Admins must sign a confidentially agreement, business associate agreement. And non-disclosure agreement. The contracts are reviewed annually by our Security SME, COR. and ISSO. For additional information about the roles, please see 8.1.c. Contractors that have been provisioned to the external box environment and verified their identity through id.me will have access to PII related to use case and data elements. Contractors with VA emails will be able to login to the environment through SSOi. All requests will use PII and PHI need go through the process of obtaining a Data Security Categorization, where the data elements are reviewed by and ISSE team member. The contractor also must complete an Acceptable Use Policy.

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.

All users must complete the following VA Training:

VA Privacy and Information Security Awareness and Rules of Behavior (WBT) (VA 10176)

VA Privacy and HIPPA Training (VA 10203)

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 08/29/2022
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 02/29/2022

5. *The Authorization Termination Date:* 08/28/2025
6. *The Risk Review Completion Date:* 08/03/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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 (please see authorization dates listed above).

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)*

Yes, the system using Google Cloud Platform. The system is a SaaS solution and has been FedRamp approved. Please see *Box VA MOU ISA-2022* for more information.

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, VA has ownership of VA data.

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.

No, the CSP will not collect any ancillary data.

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, responsibilities are described within contract language between cloud provider and organization

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).

Not applicable- The system is not utilizing Robotics Process Animation.

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.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.04.15 10:29:40 -06'00'

Privacy Officer, Julie Drake

ANNA JOHNSON Digitally signed by ANNA JOHNSON
Date: 2024.04.15 11:02:11 -07'00'

Information Systems Security Officer, Anna Johnson

HERBERT ACKERMANN Digitally signed by HERBERT ACKERMANN
Date: 2024.04.15 15:06:08 -04'00'

Information Systems Owner, Herbert Ackermann

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).

Link to Privacy Act Notice

The Box privacy notice is comprehensive and can be found in its entirety at
https://www.box.com/legal/privacypolicy

Please see below for applicable SORNs:

121VA10 / 88 FR 22112 National Patient Databases-VA 4/12/2023
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf (Legal Authority: 38 U.S.C 501)

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.federalregister.gov/documents/2022/07/01/2022-14118/privacy-act-of-1974-system-of-records
(Legal Authority: 42 U.S.C. 2165)

150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf
(Legal Authority: 38 U.S.C. 1)

172VA10 / 86 FR 72688 VHA Corporate Data Warehouse-VA 12/22/2021
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
(Legal Authority: 5 U.S.C 552)

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