Privacy Impact Assessment for the VA IT System called:

Managed Services – Loyal Source Government Services (LSGS)

Veterans Benefit Administration (VBA)

Medical Disabilities Examination Office (MDEO)

eMASS ID 2147

Date PIA submitted for review:

6/10/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	Lakisha.Wright@va.gov	202-632-7216
Information System Security Officer (ISSO)	Ronald Cox	Ronald.Cox@va.gov	414-902-5613
Information System Owner	Jennifer Treger	Jennifer.Treger@va.gov	202-461-9497

Abstract

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

Managed Services - Loyal Source Government Services (LSGS) is a single tenant managed service environment hosted on Amazon Web Services (AWS) GovCloud. The managed service is comprised of three main components (MDE4Vets, SEMOSS, and Mirth), used in support of the Medical Disability Examinations Office (MDEO) for Veterans claims processing by the Veterans Benefits Administration (VBA). LSGS supports the following functions:

(a) Disability Benefits Questionnaire (DBQ) processing: The completion and submission of DBQ's via the LSGS platform which integrates with Veterans Benefits Management System (VBMS) via Data Access Services Assessing (DAS);

(b) Workload Management: LSGS facilitates DBQ processing through a triage process of diagnostics, scheduling medical appointments, ordering laboratory & radiology tests, receiving and processing of medical exam results through HL7 data for VBMS. The end-to-end process is supported by reporting capabilities allowing for the identification and development of areas of process improvement;

(c) Case Management: The LSGS system offers provider support to Veteran customers, where providers complete web forms for DBQs, Record Reviews (RRs) and Medical Opinions (MOs). Additionally, Case Managers provide DBQ quality assurance and contention review workflow under the case management capability;

(d) Telehealth :LSGS offers audio/video conferencing telehealth options to Veteran;

(e) Billing: LSGS provides reimbursement services to veterans for approved travel costs, and invoice generation to the government.t for completed examinations and other MDEO billable items.

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?

IT System: Managed Services - Loyal Source Government Services (LSGS). Program Office: Medical Disabilities Examination Office.

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

LSGS processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans. This web application provides a secure portal for operations staff to schedule and review the quality of medical exam results, allows providers to perform and record the results of exams they perform for Veterans, and allows Veterans to track their appointments. The LSGS system supports coordination of Contract Exam Management requests and the transmission of Disability Benefits Questionnaires (DBQ) results back to the VA.

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

Loyal Source Government Services (LSGS).

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?

9000+ individuals comprising of Veterans and Providers/Clinicians.

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

LSGS system contains the following information: Veteran's first, Veteran's last name, Veteran's Date of Birth, Veteran address, Veteran's e-mail address, Veteran's Primary contact number, provider name, National Provider Information (NPI), provider address, provider email and provider contact number.
The information is collected to aid processing of exam requests from the VA VBMS systems via DAS and to manage the delivery of medical disability results to the VA for the determination of benefits for Veterans.

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

The LSGS system is comprised of three components:

- MDE4Vets: Enables LSGS to ingest patient data through ESRs, to set up appointments, review medical records, review workload of cases that, triage appointments and QA.
- SEMOSS: Semantic Open-source software used to set up appointments for veterans and to run aging DBQ reports or run reports on cases received from VA.
- MIRTH: LSGS utilizes Mirth for information management, using bi-directional sending of many types of messages and to map diagnostic tests with patients, make workflow and share patients results.

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 not applicable to LSGS. The LSGS system is hosted on AWS Gov Cloud West Region.

3. Legal Authority and SORN

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

- HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R) Part 164, Standards for Privacy of Individual Identifiable Health Information.
- Privacy Act of 1974
- 58VA21/22/28 – Compensation, Pension, Education and Vocation Rehabilitations and Employment Records - VA.
- Confidentiality of Certain Medical Records, 38 U.S.C

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?

- LSGS is covered by Privacy Act of 1974; System of Records -58VA21/22/28 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA. The SORN was reviewed on September 29, 2022, and it does cover the cloud usage or storage as it lists AWS GovCloud region in Oregon and Ohio as one of its storage locations.

4. System Changes

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

No changes to business processes will be required because of the completion of this PIA.

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

No changes in technology will be required because of the completion of this PIA.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series

(https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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: Diagnostic test result, file number, Completed Disability Benefits Questionnaires (DBQ) forms.

PII Mapping of Components (Servers/Database)

Managed Services – Loyal Source Government Services (LSGS) consists of 3 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 Managed Services – Loyal Source Government Services (LSGS) 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.

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

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
CareNet RDS	Yes	Yes	• Veteran's Name • Veteran's DOB • Veteran's e-mail address • Veteran's phone number • Completed Disability Benefits Questionnaires (DBQ) forms • Diagnostic test results • File numbers • Personal Mailing Address • Gender	To be able to ingest patient data through ESRs to set up appointments, review medical records, review workload of cases that, triage appointments and QA	Encryption of data in motion & at rest
SEMOSS RDS	Yes	Yes	• Claim Numbers • Med4Vet Unique User Identifiers	Required to set up appointments	Encryption of data in motion & at res
MIRTH DB	Yes	Yes	• Veteran Name; Veteran DOB; • Unique Identifiers, Diagnostic results	Map diagnostic tests with patients, make workflow and share patients result.	Encryption of data in motion & at res

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?

LSGS has several sources of the PII and PHI collected by the information system:

1. VA Data Access Services (DAS) Assessing system
2. Veteran Customer (via VBMS)
3. Service Providers (Quest & Trident)

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.

VA Data Access Services (DAS) Assessing system provides the LSGS system with questionnaires and medical information, while the Service Providers (Quest & Trident) provide LSGS system with Veterans diagnostic reports and test results respectively, the information together helps LSGS service portal veterans to view their claims, schedule appointments, and view examination results.

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

LSGS does not create information for external use or reporting.

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?

LSGS has several sources of the PII and PHI collected by the information system:

1. VA Data Access Services (DAS)/VBMS: Bi-lateral interconnection with DAS Assessing documented in a MOU/ISA. DAS delivers a wide range of integrally linked, complementary capabilities and services that enable the transmission of Veteran and Service Member medical, benefit, personnel and personal/administrative information (DAS data).

2. VA DBQs: LSGS examiner conducts a medical evaluation with Veterans and transcribes the evaluation outcome using the VA DQB format within the LSGS information system.

3. Diagnostic Providers: When a VA DBQ requires information needed for the VA's rating process and to complete a comprehensive evaluation, specialty diagnostics are conducted with external facilities or by an external vendor's device, that information is then transmitted securely and electronically to LSGS.

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?

LSGS does not directly collect information from veterans, data is provided to VA DAS System. LSGS is not subject to the paperwork reduction Act.

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.

PII provided in LSGS is validated at several stages - the initial stage is by the customer. The data provided by the Veteran is populated within their user account (name, address, etc.). This information can be reviewed and validated by the customer as needed and following any updates or changes.

The information and data from the VA DAS system is validated by the information system owners within the DAS system prior to being provided to the information system LSGS. If there are any errors or inconsistencies within this information the user can contact/escalate within the LSGS Customer Service /Helpdesk. Information/content provided by the service provider is initially validated by the service provider prior to sending to the LSGS system, subsequently the information is validated by the customer. If there are any errors or inconsistencies within this information the user can contact/escalate within the Customer Service helpdesk.

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?

No, LSGS does not directly collect information from veterans, data is provided to VA DAS System and transmitted securely to LSGS.

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
The LSGS system has the authority for the collection of VA and Veteran data for the purpose of the outlined system is as follows:

- HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R) Part 164, Standards for Privacy of Individual Identifiable Health Information.
- Privacy Act of 1974
- 58VA21/22/28 - Compensation, Pension, Education and Vocation Rehabilitations and Employment Records – VA.
- Confidentiality of Certain Medical Records, 38 U.S.C - Federal Information Security Management Act (FISMA)

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: Veteran's data are collected and stored in the LSGS system during account creation. LSGS IT operations team have access to the system which could lead to unintended exposure of veteran's data to systems/individuals that do not have a need or authority to access such data due to system error or a malicious actor.

Mitigation: LSGS has implemented security controls and procedures to prevent unauthorized access to Veteran data including:

- Google authenticator for MFA
- Separation of Duties (SOD).
- Use of least privilege for granting access to the information system.

Additionally, LSGS employees undergo a Rules of behavior (RoB) training which they sign at completion indicating adherence to the privacy of information they may come across while doing their job. LSGS has various mitigations in place for Privacy Risk including the fact that it is hosted within FedRAMP authorized AWS GovCloud. LSGS has also gone through the VA Authorization and Accreditation process and has an active agency Authority To Operate (ATO).

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
Veteran's Name	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used
Veteran's Date of Birth	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used
Veteran's Email Address	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used

Veteran's Phone Number	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used
Veteran's Gender	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used
Veteran's Mailing Address	Used to processes exam requests from the VA VBMS systems via DAS and manages the delivery of medical disability results to the VA for the determination of benefits for Veterans.	Not Used
Diagnostic Test Results	Schedule and review the quality of medical exam results, allows providers to perform and record the results of exams they perform for Veterans, and allows Veterans to track their appointments.	Not Used
File Number	Schedule and review the quality of medical exam results, allows providers to perform and record the results of exams they perform for Veterans, and allows Veterans to track their appointments.	Not Used
Completed Disability Benefits Questionnaires (DBQ) forms.	Coordination of Contract Exam Management requests and the transmission of Disability Benefits Questionnaires (DBQ) results back to the VA via DAS interconnection.	Not Used

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 types of data collected and produced by the information system include Veteran's Name, Veteran's Date of Birth, Veteran's email address, Veteran's phone number, Completed Disability Benefits Questionnaires (DBQ) forms, Diagnostic test results, Claim numbers. The LSGS system is not set up to perform extensive analytics on the data and information collected. Its purpose is for customer service, data centralization and scheduling for the Veteran.

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.

LSGS system does not create or make available new or previously unutilized information about veterans, but veterans are able to update their personal record if they discover an error by calling the VA support and the update will be made in coordination with LSGS.

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?

LSGS information is encrypted in transit – this is documented via VA MOU/ISA for VA interconnections, and separate contractual agreements/interconnection agreements with the service providers Trident and Quest. LSGS data is protected at rest using AES-256-bit encryption.

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

This system does not collect/store or process SSNs.

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

LSGS defines all sensitive, classified, and non-publicly available information as information that requires encryption. These are encrypted via AWS Key Management Service (KMS) or Microsoft Internet Information Services (IIS) server, which are FIPS 140-2 compliant.

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?

Access to PII data is granted using Role Based Access Control (RBAC) within LSGS. PII/PHI is protected via documented Access controls – requiring role-based permissions for administrative access – which requires approval. Additionally, access, use and modification of information/data is monitored via audit logging and monitoring processes. Prior to approval for account creation and onboarding – all users must complete required such as: Privacy and HIPAA training (TMS#: VA 10203), VA Privacy and Information Security Awareness and Rules of Behavior training (TMS#: VA 10176), Government and Public Services (GPS) Confidential Information Management Training (Team Loyal Source) and Government and Public Services (GPS) Security Training (Team Loyal Source) – additionally all users must sign an NDA before gaining access to the system.

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

LSGS documented and implemented access control policies and procedures, the documented access control policy and procedure documents addresses responsibilities of LSGS users with regards to the system. The implemented Access control for the LSGS is well documented in the approved System Security plan.

2.4c Does access require manager approval?

Access to the LSGS system is role based and requires manager approval before being granted.

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

Access to PII is protected by Access controls and modification of information/data is monitored via audit logging and monitoring processes.

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

LSGS IT Operations team

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 types of data collected, produced and retained by the information system includes: Veteran's Name, Veteran's Date of Birth, Veteran's email address, Veteran's phone number, Diagnostic test results, Completed Disability Benefits Questionnaire forms, and file number.

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.*

Specific retention timelines and destruction/disposal requirements are based on LSGS's contract with the VA.

- **Functional Acquisition Regulation (FAR) 52.212-5** --- related extract regarding record retention:

  The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

- **Performance Work Statement (PWS) Section:**

  Prior to termination or completion of this contract, Contractor will not destroy information received from VA or gathered or created by the Contractor in the course of performing this contract without prior written approval by the CO. A Contractor destroying data on VA's behalf must do so accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, and applicable VA Records Control Schedules. All data and reports shall be transferred to VBA upon contract completion.

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?

Privacy Act: VBA RCS VB–1, Part 1 Section XIII, Item 13–052.100; VBA RCS VB–1, Part I, Field in Section VII

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.

LSGS system adheres SPI elimination procedures such as collecting minimum data required for fulfilling business purposes. LSGS collects data as required for scheduling exam request, once the case is cancelled or completed, the DBQs are returned to the Government via VBMS, LSGS retains the data for 18 months after which it is erased from the system following NARA guidelines.
All claims' files folders for Compensation and Pension claims are electronically imaged and uploaded into the VBMS eFolder. Once a file is electronically imaged and established by VA as the official record, its paper contents (with the exception of documents that are on hold due to pending litigation, and service treatment records and other documents that are the property of DoD), are reclassified as duplicate—non record keeping—copies of the official record, and will

be destroyed in accordance with Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA. All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolder's are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained as historical records.
Once an electronic record has been transferred into NARA custody, the record will be fully purged and deleted from the VA system in accordance with governing records control schedules. Using commercial off the shelf (COTS) software designed for the purpose. Once purged, the record will be unavailable on the VA system, and will only be accessible through NARA.
Prior to destruction of any paper source documentation reclassified as duplicate copies, VA engages in a comprehensive and multi-layered quality control and validation program to ensure material that has been electronically imaged is completely and accurately uploaded into the VBMS eFolder. To guarantee the integrity and completeness of the record, VA engages in industry-best practices, using state-of-the-art equipment, random sampling, independent audit, and 100% VA review throughout the claims adjudication process. Historically, VA's success rate in ensuring the accuracy and completeness of the electronic record routinely and consistently exceeds 99%. Furthermore, no paper document is ever destroyed while any related claim or appeal for VA benefits is still pending. VA waits 3 years after the final adjudication of any claim or appeal before destroying the paper duplicate copies that have been scanned into the VBMS eFolder. As noted, the electronic image of the paper document is retained indefinitely as a permanent record either by VA or NARA.
Decisions to destroy VR&E paper counseling records are to be made in accordance with Records Control Schedule (RCS), RCS VB–1, Part I, Field in Section VII, dated January 31, 2014.
Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA.
Education file folders in paper are retained at the servicing Regional Processing Office. Education paper folders may be destroyed in accordance with the times set forth in the VBA Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.
Employee productivity records are maintained for two years after which they are destroyed by shredding or burning. File information for CAIVRS is provided to HUD by VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes

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.

LSGS system does not use the information/data collected for research, testing or 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: PII data is only required for transactional and audit purposes and transactional usage and should only be retained for about 20 days for transactional purposes, keeping data past the required period and use creates unnecessary use and unintended exposure to users that may not need to have access to such PII data.

Mitigation: LSGS has implemented data handling procedures to take care of transactional uses of data and audit usage. For data in transactional state – Access control methods including MFA and Virtual access control are in place to ensure that only authorized LSGS users that have gone through the background check and security and compliance training and required to have access to the LSGS system could potentially have access to Privacy data. All LSGS contractors are required to sign a non-disclosure agreement. Policies and procedures such as data archiving or disposal are also in place to guide the use of auditable data.

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 DAS Assessing	LSGS receives and shares information for DBQs	• Veteran's Name • Veteran's DOB • Veteran's e-mail address • Complete Disability Benefits Questionnaires (DBQ) forms • Diagnostic test results • File numbers • Personal Mailing Address • Gender	All vendor traffic goes over the Internet through the Trusted Internet Connection (TIC) gateway on port 443. LSGS transfers the Veteran data in Health Level 7 (HL7) format to the VA using a FIPS 140-2 compliant web services call (HTTPS) supported with SSL certificates and is

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*
			encrypted in transit.

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: Unintended exposure of PII data to personnel that ordinarily should not have access to such data.

Mitigation: Data sharing between DAS and the VA is done securely and LSGS has a MOU/ISA in place which guides the sharing and transfer of data.

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 be more than one)***	***List the method of transmission and the measures in place to secure data***
Trident	Veteran Test Results	Veteran Test Results	Contractual/Interconnection agreement between LSGS and Trident	All vendor traffic goes over the internet through the Trusted Internet Connection (TIC) gateway on port 443. The secure interconnection is set up to be unilateral (in-bound only).
Quest	Veteran Diagnostic Reports	Veteran Diagnostic Reports	Contractual/Interconnection agreement between LSGS and Quest	All vendor traffic goes over the internet through the Trusted Internet

				Connection (TIC) gateway on port 443. The secure interconnecti on is set up to be unilateral (in-bound only).

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: When sharing information to external organizations, the likelihood of a data breach increases as a result of a larger attack surface and the potential for third-party breaches that could result in compromised data. Breaches in data can lead to the loss of PII and cause operational disruptions.

Mitigation: LSGS does not share data to external organizations, external connections are unilateral (inbound), and data is provided to LSGS. Additionally, there are technical measures in place to mitigate the risk of data getting into the hands of unintended users such as the use of HTTPS interfacing, HL7 over MLP, IPSEC VPN Tunnel and application whitelisting. We also have a MOU/ISA agreement between LSGS and DAS. There are also agreements with LSGS service providers such as Quest and Trident that only allows a one-way connection into LSGS system by design.

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.
58VA21/22/28 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA.

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

Privacy data is collected by the VA VBMS system, LSGS does not directly collect PII from Veterans.
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

Not applicable to LSGS. LSGS does not directly collect veterans' information. Veteran's data is collected by VA VBMS and sent to LSGS for processing. LSGS has a VA DAS MOU/ISA for secure transmission of data via interconnection.

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.

Not applicable to LSGS. LSGS does not directly collect veterans' information. Veteran's data is collected by VA VBMS and sent to LSGS for processing. LSGS has a VA DAS MOU/ISA for secure transmission of data via interconnection.

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.

Not applicable to LSGS. LSGS does not directly collect veterans' information. Veteran's data is collected by VA VBMS and sent to LSGS for processing. LSGS has a VA DAS MOU/ISA for secure transmission of data via interconnection.

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: LSGS does not directly collect PII data from Veterans; therefore, Veterans will not know how their information is being used.

Mitigation: The SORN, via VBMS, published provides notice to veterans about how this information is used.

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.

Veterans can access their information in the system at any time following the creation of a user account by simply logging back into their portal. If there are questions, escalation, or concerns regarding service the user can contact the escalation/customer service support team via dialing 833-832-7077 or 720-449-8003.

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)?

Not applicable to LSGS. LSGS does not collect data from Veterans. Veteran data is directly collected by VA DAS Assessing. LSGS has a VA DAS MOU/ISA for secure transmission of data via interconnection.

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?

Veterans can access their information in the system at any time following the creation of a user account by simply logging back into their portal. If there are questions, escalation, or concerns regarding service the user can contact the escalation/customer service support team via dialing 833-832-7077 or 720-449-8003.

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.

Whenever there is inaccurate information regarding authoritative data such as medical information, LSGS will contact the VA for clarification through the escalation/customer service support team. If the inaccurate or erroneous information is regarding demographic data, LSGS will reach out to the veteran for clarification and correction.

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.

LSGS does not directly collect veterans' information. Veteran's data is collected by VA VBMS and sent to LSGS for processing. In the event of incorrect data being sent to LSGS, LSGS will

analyze the situation and immediately remove the data from its system and inform the VA accordingly.

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 will be coordinated with the VA and sent back to LSGS for rework/clarification/update.

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: When veterans enter their data in the VBMS system and the data is sent to LSGS system, there is a risk that the veteran could input incorrect data, which would in turn get sent to other LSGS 3rd Party systems such as DAS. Some veterans might notice they have an incorrect data in the system but may fail to contact VA support to correct their information.

Mitigation: Veterans have access to their data by logging into their portal. They can request update or correction by coordinating with the VA support and LSGS, if request is valid, and after proper triage and analysis, the update will be made.

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?

LSGS has documented Access Control policies in place to ensure that only authorized users can access the system. LSGS has privileged and non-privileged accounts and has implemented Role Based Access Control (RBAC) and least privilege principles which limits the system use to only authorized users and LSGS system users are only provided privileges required to perform their given task. For users to gain access to the LSGS system, they must go through an onboarding process which includes background check and Security and Awareness training.

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?

Users from other agencies such as DAS do not have access to the LSGS system.

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.

LSGS has created Privileged and non-privileged roles for the different types of users in the system and were granted permission accordingly.

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.

LSGS system is a Managed Service maintained by Loyal Source, supporting VA Medical Benefit Examination (MDE). Contractors working for LSGS are required, prior to gaining access to the system, to sign a Non-Disclosure Agreement (NDA) as well as complete a criminal background check.

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 LSGS system users are required to take annual security training including the following: Privacy and HIPAA training (TMS#: VA 10203), VA Privacy and Information Security Awareness and Rules of Behavior training (TMS#: VA 10176), Government and Public Services (GPS) Confidential Information Management Training (Team Loyal Source) and Government and Public Services (GPS) Security Training (Team Loyal Source).

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

8.4a If Yes, provide:

1. *The Security Plan Status: Completed*
2. *The System Security Plan Status Date:* 02/29/2024
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 05/10/2024
5. *The Authorization Termination Date:* 05/10/2025
6. *The Risk Review Completion Date:* 05/08/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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)*

LSGS is hosted on Amazon Web Services (AWS) GovCloud (US) High Assessing with a FedRAMP Authorization.

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.*

Section 16F - PROPRIETARY INFORMATION AND DATA of contract# 36C10X22D0011 between LSGS and the VA has the following statement therein: The VA shall retain sole rights in all deliverables, reports, correspondence, or other documents in any media produced as a result of this contract.

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 CSP does not collect or have access to veteran's 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.

The AWS Shared Responsibility model that states that the customer is responsible for security of the data in the cloud is embedded in contracts with AWS and LSGS

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).

LSGS will use RPA agents to automate routine tasks for internal users of the LSGS system. All RPA solutions will be deployed locally and operate in an unattended mode. LSGS will be using these primarily to do the following:

- Automate the collection of internal data to create CSVs to create user accounts.
- Automate scheduling processes otherwise performed by a user within the system.

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 they provided in this Privacy Impact Assessment is true and accurate.

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.07.11 15:10:39 -04'00'

Privacy Officer, Lakisha Wright

RONALD COX

Digitally signed by RONALD COX
Date: 2024.07.12 07:01:48 -05'00'

Information System Security Officer, Ronald Cox

JENNIFER TREGER

Digitally signed by JENNIFER TREGER
Date: 2024.07.12 12:53:18 -04'00'

Information System Owner, Jennifer Treger

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.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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