



Privacy Impact Assessment for the VA IT System called:
Salesforce: VA National Telestroke Program (NTSP) CRM Module

Date PIA submitted for review: 1/25/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-870-1284
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	267-283-7653
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-482-1398

Abstract

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

VA National TeleStroke Program (NTSP) serves veterans with acute stroke symptoms at VA emergency departments, urgent care centers, and hospitals. It offers acute stroke expertise to VA facilities that lack around-the-clock acute stroke coverage. This solution will serve as a streamlined way for Veterans Affairs Medical Centers (VAMCs) to virtually connect with Stroke Specialist and provide exceptional care to veterans that may be experiencing stroke related symptoms. This will allow the National TeleStroke Program to intake urgent stroke patient incidents and ensure they receive the best treatment possible in a timely manner. This will allow NTSP to efficiently intake veteran stroke incidents and efficiently route to TeleStroke Neurologists to provide necessary care. This system will completely streamline the processing allowing for automatic routing, triage, and treatment within the required SLA's. It will also give NTSP Leadership visibility across to program to better measure their effectiveness and Veteran impact.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Salesforce: VA National Telestroke Program (NTSP) CRM Module serves veterans with acute stroke symptoms at VA emergency departments, urgent care centers, and hospitals. It offers acute stroke expertise to VA facilities that lack around-the-clock acute stroke coverage. The expected number of individuals is currently indeterminate but is expected to be only the subset of VA users requiring stroke care. Exact number to be determined (TBD). This solution will serve as a streamlined way for VAMC's to virtually connect with Stroke Specialist and provide exceptional care to veterans that may be experiencing stroke related symptoms. This will allow the National TeleStroke Program to intake urgent stroke patient incidents and ensure they receive the best treatment possible in a timely manner. This will allow NTSP to efficiently intake veteran stroke incidents and efficiently route to TeleStroke Neurologists to provide necessary care. System will be operated from one location, within Salesforce Gov Cloud Plus per architectural depiction. This system will completely streamline the processing allowing for automatic routing, triage, and treatment within the required SLA's. It will also give NTSP Leadership visibility across to program to better measure their effectiveness and Veteran impact. Michael Domanski is the ISO for the system. A SORN exists for this system and is up to date. Data shared will include the data elements listed in section 1.1 and the transitory data elements of the VA-VET ORG Database.

Although the system data is stored in the Salesforce FedRAMP Government Cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF Process, the system has a Data Categorization of High, with the impacts of a data compromise being identified in the Data Security Categorization (DSC) memo. The Privacy Act is the legal authority to utilize this information. The system will not cause any business processes to change, cause any technology changes, nor affect the relevant SORN applicable for the system mentioned below. The SORN covers all Personally Identifiable Information (PII) used.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Financial Account Information | <input checked="" type="checkbox"/> Medical Record Number |
| <input checked="" type="checkbox"/> Social Security Number | <input type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Gender |
| <input checked="" type="checkbox"/> Date of Birth | <input type="checkbox"/> Account numbers | <input type="checkbox"/> Integration Control Number (ICN) |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Certificate/License numbers | <input type="checkbox"/> Military History/Service Connection |
| <input type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Next of Kin |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | <input checked="" type="checkbox"/> Other Unique Identifying Information |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Current Medications | |
| <input type="checkbox"/> Personal Email Address | <input type="checkbox"/> Previous Medical Records | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Race/Ethnicity | |
| | <input type="checkbox"/> Tax Identification Number | |

Consult date, local time 24hrs, last known well, facility, triaged, location, telestroke staff, outcome, diagnosis, TPA administered, 24 hr. follow up needed, process difficulties, notes, description of process difficulties, length of call with facility, Name & role of caller, local time of call, facility (city & state), department (ED or inpatient), Dr caring for patient and stroke symptoms.

PII Mapping of Components

VA National Telestroke Program- CRM Module consists of one key component (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA National Telestroke Program and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
--	--	--------------------------------------	------------------------------	---------------------------------------	------------

VA-VET ORG Database	Yes	Yes	Last name, last four SSN, Consult Date, local time 24hrs, last known well, facility, triaged, location, telestroke staff, outcome, diagnosis, TPA administered, 24 hr. follow up needed, process difficulties, notes, description of process difficulties, interesting case, interesting case, interesting case, interesting case discussed, length of call with facility, Name & role of caller, local time of call, facility (city & state), department (ED or inpatient), Dr caring for patient and stroke symptoms.	This solution will serve as a streamlined way for VAMC's to virtually connect with Stroke Specialist	MOU/ISA Encrypted Transmission
---------------------	-----	-----	---	--	--------------------------------

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The sources of information come from the VA-VET ORG Database as a point of data consumption.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The sources of information are received from the VA-VET ORG Database. Informational connection from the VA-VET ORG is utilized to provide an accurate data pathway of veteran information, delineated into a subset of stroke user data, to provide accurate and timely care to the veterans using the system.

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

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.

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

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

There are no system checks. The manager role of the solution is responsible for maintaining data integrity.

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

SORN 24VA10A7 Patient Medical Records–VA provides authority for the operating system. https://www.oprm.va.gov/docs/Current_SORN_List_1_7_2022.pdf

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.

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: Due to sensitive data store in this system, there is risk that, if the data were accessed by an unauthorized individual or otherwise breached this could result in serious harm including

identity theft. Important staffing information is located in this system and employee's names service line, and occupational series are listed in the system.

Mitigation: All PII will be processed and sent using a MOU/ISA encryption.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

The information in this system will be used to virtually connect Veterans Administration Medical Center (VAMC) stroke patients to specialists. The following data elements are used for the specific purpose of providing medical care to the veteran

Name – Specific Purpose= Identification of Veteran

Social Security Number- Specific Purpose= Identification of Veteran

Date of Birth- Specific Purpose= Identification of Veteran

Personal Phone Number- Specific Purpose= Identification of Veteran

Medical record number- Specific Purpose= Identification of Veteran

Consult date- Specific Purpose- Identification of Veteran, record of care received

local time 24hrs-Specific Purpose= Identification of Veteran, record of care received.

last known well- Specific Purpose= Identification of Veteran, record of care

facility- Specific Purpose= Identification of Veteran, record of care

triaged- Specific Purpose= Identification of Veteran, record of care

location-Specific Purpose= Identification of Veteran, record of care

telestroke staff- Specific Purpose= Identification of Veteran, record of care

outcome- Specific Purpose= Identification of Veteran, record of care

diagnosis- Specific Purpose= Record of care

TPA administered- Specific Purpose= Record of care

24 hr. follow up needed- Specific Purpose= Record of care

process difficulties- Specific Purpose= Record of care

notes- Specific Purpose= -Record of care received

description of process difficulties- Specific Purpose= -Record of care received

length of call with facility- Specific Purpose= -Record of care received

Name & role of caller- Identification of veteran/caretaker

local time of call- Specific Purpose= -Record of care/support received

facility (city & state) Specific Purpose= -Record of care received

department (ED or inpatient)- Specific Purpose= -Record of care received
Dr caring for patient and stroke symptoms-Record of care

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

VA-VET ORG database will be utilized in this system. The data it analyzes will help with human capital management. These analyses are performed to mitigate the issue of VAMCs having to request additional staff from one another and can instead find someone within their office that could assist with a problem or absence of an individual. No New information is created about individuals

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

The information is stored within VA-VET ORG Database in Salesforce. Control Implementation will be based on at least FedRAMP Moderate impact. FedRAMP moderate impact controls are used to protect data in transit and at rest. SSNs encrypted by Salesforce Shield Protect, which provides FIPS 140-2 certified encryption

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Mitigation:

- NTSP adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- All internal employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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

Last name, last four SSN, Consult Date, local time 24hrs, last known well, facility, triaged, location, telestroke staff, outcome, diagnosis, TPA administered, 24 hr. follow up needed, process difficulties, notes, description of process difficulties, interesting case, interesting case discussed, length of call with facility, Name & role of caller, local time of call, facility (city & state), department

(ED or inpatient), Dr caring for patient and stroke symptoms are included in this system in order to help manage Veterans Integrated Services Networks(VISNs).

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.*

Information is to be retained temporarily in the VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record. Per item number 6000.1 Health Records Folder File or CHR (Consolidated Health Record).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

*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.
This question is related to privacy control DM-2, Data Retention and Disposal.*

The retention guidelines have been provided by the Records Management Office. The retention [schedule is 6000.2](#) Health Records Folder File or CHR (Consolidated Health Record).

3.4 What are the procedures for the elimination of SPI?

*Explain how records are destroyed or eliminated at the end of the 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*

After 3 years since last episode of care files are convert to an inactive medical record and destroyed or deleted after 75 years after the last episode of patient care per 6000.2b.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Yes, it does, for SSNs the system uses Salesforce Shield Protect as a control implemented to protect PII used for testing and training, which provides FIPS 140-2 certified encryption. Access to all data is controlled by employees' roles and function, this minimizes the amount of risk.

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.

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: Records held longer than the required time are at greater risk of being unintentionally released or breached and this may result in identity theft among other relevant concerns. This system only stores PII on employee's name, occupational series, and service line. This minimizes the amount of PII that is at risk if the system were to be breached.

Mitigation: The information may be retained in accordance with existing DTC Salesforce guidelines. NTSP has an MOU/ISA in place with DTC Salesforce to enforce the Encryption of

Data at Rest or retention and Transmission. This process of Encryption prevents the data breach or spillage.

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?

This system only uses data from the VA-VET ORG database. There is no other sharing of information with other internal systems.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VA-VET ORG Database	This solution will serve as a streamlined way for VAMC's to virtually connect with Stroke Specialist	Last name, last four SSN, Consult Date, local time 24hrs, last known well, facility, triaged, location, telestroke staff, outcome, diagnosis, TPA administered, 24 hr. follow up needed, process difficulties, notes, description of process difficulties, interesting case, interesting case discussed, length of call with facility, Name & role of caller, local time of call, facility (city & state), department (ED or inpatient), Dr caring for patient and stroke symptoms	All data that is sent from this system is sent through encrypted transmission

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.

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

Follow the format below:

Privacy Risk: There is a minor to no risk since all data is encrypted before transmission.

Mitigation: All data that is sent from this system is sent through encrypted transmission.

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: No risk, as no information is externally shared by this system.

Mitigation: No information is externally shared by this system.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

The Department of Veterans Affairs provides additional notice of this system by publishing System of Record Notices (SORN): The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN24VA10A7 (Oct 2nd, 2020), in the Federal Register and online. An online copy of the SORN can be found at: <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf> .

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, they do have the option. No penalty or denial of service is associated. Subsequently, the information collected/used is required for the intended use, so in the event the information is not supplied, the individual would be unable to use the system.

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

These individuals are made aware of why data is collected through the Notice of Privacy Practices (NOPP) and conversations with employees. VA Forms are reviewed periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals.

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.

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

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

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the VAMC.

Mitigation: Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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?

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.

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).

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 question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

All data used is originating from the VA-VET database. Access to their data can be requested by contacting the VA-VET ORG database owner or the NTSP system owner or the designated POCs.

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.

All questions concerning erroneous information or corrections should be directed to the system administrator or VA-VET ORG system owner.

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.

All questions concerning erroneous information or corrections should be directed to the system administrator or VA-VET ORG system owner

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.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

All questions concerning erroneous information or corrections should be directed to the system administrator or VA-VET ORG system owner

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.

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: Currently there are no known privacy risk that exists in the system. Individuals have the right to decline to provide their information to the NTSP; however, without providing the information NTSP cannot provide the needed care for the Veteran. The Veteran is given a written statement or notice detailing reasons of denial of access and or correction with guidance on to appeal the decision.

Mitigation: A privacy notice is given to the user as stated in Section 6.1 on the VA Handbook 6500, that states that the system exists in detail, along with the Privacy Act Statement of Records Notice. All the information provided during the application is validated through the submission of documentary evidence provided by the Veterans.

All the information provided during the application is validated through the submission of documentary evidence provided by the Veterans. The NTSP review all eligibility requests and records them. Additionally, records are reviewed for quality assurance purposes. These audits include a review of the original application submitted by the Veteran, correspondence logs, relevant documentary evidence, and information in existing VA systems and are used for no other than the purpose obtained for.

The NTSP review all eligibility requests and records them. Additionally, records are reviewed for quality assurance purposes. These audits include a review of the original application submitted by the Veteran, correspondence logs, relevant documentary evidence, and information in existing VA systems and are used for no other than the purpose obtained for.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access is granted based on a least privilege basis, dependent the level and role of the user, and use case. Acceptable Use Policy (AUP) documentation is utilized for the purposes of documentation and resides with the VA-VET ORG Database. Please contact system admin for copies of documentation/AUP.

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.

Yes. When and where there is a need for contractor access, an NDA will be used.

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.

Users are required to take security privacy and HIPPA trainings.

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

If Yes, provide:

- 1. The Security Plan Status,*
- 2. The Security Plan Status Date,*
- 3. The Authorization Status,*
- 4. The Authorization Date,*
- 5. The Authorization Termination Date,*
- 6. The Risk Review Completion Date,*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The FIPS 199 classification of the system is HIGH (C/I/A – M/H/H). The National Telestroke Program falls under the Salesforce Government Cloud Plus -Enterprise (SFGCP -E) ATO. The ATO process is in flight - IOC 5/1/2022. Currently in RMF Step 1

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).

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.

Yes, this system utilizes data from the VA-VET ORG database. The system is built on the salesforce development platform which is in the VA Enterprise Cloud.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

n/a

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, there is no 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, Salesforce operates the system, and the VA owns it. This system agreement is stated in the Cloud Service Provider Agreement.

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).

No RPA is used in this 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

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

Signature of Responsible Officials

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

Privacy Officer, Rita Grewal

Information Systems Security Officer, James Boring

Information Systems Owner, Michael Domanski

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).

The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN24VA10A7 (Oct 2nd, 2020), in the Federal Register and online. An online copy of the SORN can be found at:

<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>