Privacy Impact Assessment for the VA IT System called:

Alexsys Team

National Data Systems

Veterans Health Administration

Date PIA submitted for review:

08/17/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly E. Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Peter Pol G. Tadalan	Peterpol.Tadalan@va.gov	916-212-4227
Information System Owner	Jim Peterson	James.Peterson2@va.gov	727-432-6685

Abstract

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

Alexsys Team is a commercial off the shelf product (COTS) product (http://alexsys.team) used by National Data Systems (NDS) for workload tracking, help desk activities, and tracking of national access to the Veterans Health Information Systems and Technology Architecture (VistA) Compensation and Pension Records Interchange (CAPRI), VistA Remote Access Management (VRAM), and Joint Legacy Viewer (JLV) applications. Alexsys Team is approved on the VA Technical Reference Model (TRM) (http://trm.oit.va.gov/ToolPage.asp?tid=7243) and has not been altered in any way. The system is internal to NDS, whose staff enter data into the system. Data entered into the system is only viewed by NDS staff.

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?*

Alexsys Team is used by National Data Systems (NDS) for workload tracking, help desk activities, and tracking of national access to the Veterans Health Information Systems and Technology Architecture (VistA) Compensation and Pension Records Interchange (CAPRI) and VistAWeb applications. Alexsys Team is approved on the TRM (http://trm.oit.va.gov/ToolPage.asp?tid=7243) and has not been altered in any way.

Alexsys Team is internal to NDS. Data is entered by NDS staff and only viewed within NDS.

Teamlog is the back-end database for Alexsys Team. The database is located in the Health Administration Center's data center in Region 1.

An average of 15,753 rows are added to the Teamlog database each year. The Teamlog database is on a Structured Query Language (SQL) Server within Region 1. The employee enters information in the Teamlog database which includes VA Employee's name, work phone number, work email address, network ID and domain, station number, Information System Security Officer (ISSO) and Supervisor Email, job title, purpose of use for access, data sources (type of access) authorized, employee type, contracting company and address if a VA contractor. There is no information sharing. The system is only operational at 1 site.

The Legal authority to collect privacy information is maintained under the System of Records Notice 79VA10P2, Veterans Health Information System and Technology Architecture (VistA) Records-VA (Published in the Federal Register on October 31, 2012) AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a). link: https://vaww.vets.vaco.portal.va.gov/sites/privacy/Update_SOR/79VA10P2-VistA_Records-VA.pdf. 150VA19, Administrative Data Repository—VA'' (Published in the Federal Register on November 26, 2008. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.and Section 7304. Link: https://www.gpo.gov/fdsys/pkg/FR-2008-11-26/pdf/E8-28183.pdf. OPM/GOVT-1, General Personnel Records (Published in the Federal Register on June 19, 2006) AUTHORITY FOR MAINTENANCE OF THE SYSTEM:5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107. Link: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570733/opmgovt-1/

Currently there will be on technology changes affected by this PIA. Completion of this PIA will not result in technology changes. The SORN will not require amendment. This data collection does not use cloud services for operation or storage. This data collection does not use cloud services for operation or storage.

The magnitude of harm would be relatively low, or none at all, since the system does not provide more that the employee name and email address that relates to the individual identity. This data collection is used internally to the VA to process IT tickets. Government employee data is not PII/PHI

Section 1. Characterization of the Information

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

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

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

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

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

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

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

VA Employee's work phone number, work email address, network ID and domain, station number, Information System Security Officer (ISSO) and Supervisor Email, job title, purpose of use for access, data sources (type of access) authorized, employee type, contracting company and address if a VA contractor

PII Mapping of Components

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

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

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**
teamlog	Yes	Yes	Name, work phone number, work email address, network ID & domain	Collected data is required in order to provide national access to CAPRI and VistAWeb	Access to the database and user interface has only been given to NDS staff. SQL database is encrypted.
TeamLog_Dev	Yes	Yes	Name, work phone number, work email address, network ID & domain	This is a copy of the production database that is used for testing of changes to the user interface	Access to the database and user interface has only been given to NDS staff. SQL database is encrypted.

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.

Data elements collected regarding VA employees is hand entered by NDS staff (VA employees) using the user interface provided by Alexsys Team. The data is obtained from an Electronic Permission Access System (ePAS) form (VHA NDS Access Form for Health Operations) that is submitted by the individual in order to obtain national access to CAPRI and VistAWeb.

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.

All data is hand entered by NDS staff using the user interface provided by Alexsys Team. The data is obtained from an ePAS form (VHA NDS Access Form for Health Operations) that is submitted by the individual in order to obtain national access to CAPRI and VistAWeb.

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 automated mechanisms in place for checking the data for accuracy. Accuracy checks are done manually by NDS staff by comparing the data that was entered into Alexsys Team against the data that was provided by the individual in ePAS.

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 Legal authority to collect privacy information is maintained under the System of Records Notice 79VA10P2, Veterans Health Information System and Technology Architecture (VistA) Records-VA (Published in the Federal Register on October 31, 2012) AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a). link: https://vaww.vets.vaco.portal.va.gov/sites/privacy/Update_SOR/79VA10P2-VistA_Records-VA.pdf

150VA19, Administrative Data Repository—VA'' (Published in the Federal Register on November 26, 2008. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.and Section 7304. Link: https://www.gpo.gov/fdsys/pkg/FR-2008-11-26/pdf/E8-28183.pdf

OPM/GOVT-1, General Personnel Records (Published in the Federal Register on June 19, 2006)
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107. Link: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570733/opmgovt-1/

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> The information collected and stored in the database is not accurate or relevant to the business process. Information received from the VA employee is not accurate.

<u>Mitigation:</u> Incorrect information can be corrected by National Data Systems (NDS) when it is identified as being incorrect. Information that is not relevant to the business process can also be removed by NDS when it is identified..

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 data collected is used to establish national access to CAPRI and VistAWeb. The requestor would complete an ePAS form, which the requestor signs and the supervisor signs. Based on the ePAS form, NDS would process the request which would result in an entry being made into the Alexsys system.

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

Reports being utilized to provide totals for the number of entries created and do not contain any data about the individual. These reports are not automated and are run manually at the end of each month.

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

Alexsys Team is used by National Data Systems (NDS) for workload tracking, help desk activities, and tracking of national access to the Veterans Health Information Systems and Technology Architecture (VistA) Compensation and Pension Records Interchange (CAPRI) and VistAWeb applications. No PII/PHI is collected and that it uses the VA Baseline, FIPS 140-2 encryption for data at rest and during in transit.

Alexsys Team does not have any external connections and it is using VA's General Support Systems that are FIPS 140-2 compliance (encrypted).

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.

Add answer here:

Access is only granted to team members of National Data Systems (NDS) that have a need to view or enter data to manage access. Several Standard Operating Procedure (SOP)s are in place that provides guidance on the criteria, procedures, controls, and responsibilities. The supervisor must approve access for team members to access this system. NDS does maintain a list of who has access which is reviewed. Access to Alexsys Team has only been provided to the NDS team. NDS staff that are not involved with the establishment of national access to CAPRI and VistAWeb have not been given access.

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

VA Employee’s name, work phone number, work email address, network ID and domain, station number, ISSO and Supervisor Email, job title, purpose of use for access, data sources (type of access) authorized, employee type, contracting company and address if a VA contractor. Information populated by User interface (i.e. hand entered) NDS team members from the work tickets the employee enters.

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.

2000.7. Help desk services are provided by service centers to respond to government and contract employees' technical and administrative questions. This schedule covers records on managing administrative, technical, and information technology (IT) help desk. It includes records on assistance provided both within the agency and through inter-agency service agreements on functions such as IT help, security, parking, payroll, timekeeping, human resources, etc.
Technical and Administrative Help Desk Operations records.

- □ records of incoming request (and responses) made by phone, email, web-portal, etc.
- □ trouble tickets and tracking logs
- □ quick guides and "Frequently Asked Questions" (FAQ's)
- □ evaluations and feedback about help desk services
- □ analysis and reports generated from customer management data
- □ customer/client feedback and satisfaction surveys, including survey instruments, data, background material, and reports

Temporary; destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. (GRS 5.8 item 010, DAA-GRS-2017-0001-0001)

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.

Yes, VHA Record Control Schedule 10-1 at: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

Alexsys Team data is not currently purged or archived. This is because NDS will be asked if we provided national CAPRI access to someone (i.e. it's our record of who we provisioned access for) and we also use the information for workload tracking/trending.

When business use is determined that data is no longer needed the entered information is removed (deleted) by a VA employee in accordance with the VHA Records Control Schedule 10-1. Temporary; destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. (GRS 5.8 item 010, DAA-GRS-2017-0001-0001)

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

Test PII data (ex: Mickey Mouse) was used for initial configuration testing and removed prior to deployment to the production environment.

Training of new users is done on the production system after the user has obtained their VA credentials.

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: If data is maintained within Alexsys Team for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation: Access to Alexsys Team has been limited to members of the NDS team that have a need to view or enter data when provisioning and managing national access to CAPRI and VistAWeb. Team members access the data through the GUI front end provided by Alexsys Team and are not able to directly access the back-end Teamlog database (ex: SQL Server Management Studio), unless they have explicitly been given administrative access (aka elevated privileges) to it. Only members of the NDS team [with a need to access Alexsys Team] have been given access. The Alexsys Team system does not electronically share/transmit the data contained within it with any other database.

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***
N/A			

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: The data is accessed by a VA employee without a need to know or the proper credentials.

Mitigation: Access is only provided to VA Employees that have a need to know and are members of National Data Systems. Annual awareness training for all VA employees and contractors is required.

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***
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: N/A

Mitigation: N/A

A privacy risk is not applicable since Alexsys data is not accessible by unauthorized personnel outside the VA.

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.

Privacy notices are provided in the following ways:

This Privacy Impact Assessment (PIA) also serves as notice of the system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

Veterans, Beneficiaries and VA employees: 79VA10P2, Veterans Health Information System and Technology Architecture (VistA) Records-VA
Veterans, Beneficiaries and VA employees: 150VA19, Administrative Data Repository—VA''
(Published in the Federal Register on November 26, 2008. VA employees: OPM/GOVT-1, General Personnel Records (Published in the Federal Register on June 19, 2006)

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

VA employees are required to provide information necessary for the Office of information Technology may use to verify access privileges. If adequate information to process the work ticket or it does not contain the supervisor approval, the process will not be completed, and such action will be documented in the data collection.

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

VA employees are required to provide information necessary for the Office of information Technology may use to verify access privileges. Employees are provided their job parameters when hires, in performance appraisals, submitting a IT ticket for system access is outlined in their job duties.

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: Persons are not made aware of their rights before providing personal information.

Mitigation: Users are not providing information directly to this system. Information is provided to an ePAS form which is then populated into this system. Our ePAS form does provide the FOIA notice.

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.

The information they provided is located on the ePAS form they filled out. The ePAS system will allow them to view the information they submitted after they completed the form. The ePAS system provides notices to complete and update the form.

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

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

If a VA employee identifies their information is incorrect they will contact the Office of Information Technology to update. If an error is identified by OIT the VA OIT personnel will work with the VA employee to gather and update the information.

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.

Users would reach out to our team based on correspondence (email) from providing access based on the information they provided on the ePAS form. We also have a VHA Data Portal website which provides information on how to contact our team with issues regarding their access.

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 ensures data accuracy.

A VA employee can request a copy of their access through the Privacy Office. This is completed by emailing vha.occ.po@va.gov. This system does not have the ability to allow users to directly access and correct/update their information online. If the information is discovered to be incorrect, a VA employee with access will make the needed corrections.

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: Information in the database is incorrect, and OIT used that information to make access decision. Incorrect or elevated access was granted using incorrect information.

Mitigation: NDS does provide access from the ePAS form that the user submits. If the information in the data collection is incorrect the VA employee would not gain access to the systems they need, and would submit a new request for access.

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.

Only members of the NDS team are provided access to Alexsys Team 2 Pro. NDS team members that have been provided access have the ability to add/edit/view all data.

One NDS team member has been given elevated privilege access (via their NEMA account) to the Teamlog database for the purpose of system maintenance. Two NDS team members have been given read-only access to the Teamlog database for the purpose of generated summary reports [that contain no PII/PHI data]. All other NDS users accessing the system do so through the user interface provided by Alexsys Team.

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. Contractors are internal to the VA and are required to comply with Information Security requirement, that utilize the system and access data in the VA network. The contractors do not design and maintain the system. The primarily enter data into the system as an end user. This contract is being maintained by the COR.

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 NDS team members complete the yearly VA Privacy and Information Security Awareness training (TMS course VA 10176) and Privacy and HIPAA Focused training (TMS course VA 10203).

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training

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.***

Alexsys Team went through the Authorization and Assessment process on November 27, 2021 and received an approval of 3-year recommendation on December 1, 2021.

The following information is in support of this approval:

1. The Security Plan Status – Approved

2. The Security Plan Status Date – August 12, 2021

3. The Authorization Status – Authorization to Operate (ATO)

4. The Authorization Date – December 1, 2021

5. The Authorization Termination Date – November 30, 2024

6. The Risk Review Completion Date – November 16, 2021

7. The FIPS 199 Classification is Moderate

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.

Cloud technology is not used.

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 (cloud technology is not used)

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.

N/A (cloud technology is not used)

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.

N/A (cloud technology is not used)

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).

Robotics Process Automation (RPA) is not used.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E.
Murphy 183320
Date: 2022.09.06 14:04:22 -04'00'

Privacy Officer, Kimberly E. Murphy

PETER POL G.
TADALAN 637890

Digitally signed by PETER POL
G. TADALAN 637890
Date: 2022.09.07 15:00:19
+08'00'

Information System Security Officer, Peter Pol G. Tadalan

James R.
Peterson 356007

Digitally signed by James R.
Peterson 356007
Date: 2022.09.06 11:37:55 -04'00'

Information System Owner, Jim Peterson

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).

23VA10NB3: Non-VA Care (Fee) Records (Published on July 30, 2015)

54VA10NB3: Veterans and Beneficiaries Purchased Care Community Health Care Claims,

Link to ePAS form: https://epas.r02.med.va.gov/submit.cfm?action=select&doc_type=690