Privacy Impact Assessment for the VA IT System called:

National Utilization Management Integration (NUMI)

Health Product Support

Veterans Health Administration

Date PIA submitted for review:

4/28/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Joseph Facciolli	joseph.facciolli@va.gov	215-842-2000 x2012
Information System Owner	Jeffrey Rabinowitz	Jeffrey.Rabinowitz@va.gov	7327205711

Abstract

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

The National Utilization Management Integration (NUMI) application is a Web-based solution that automates documentation of clinical features relevant to each patient's condition and the associated clinical services provided as part of VHA's medical benefits package.

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*

The National Utilization Management Integration (NUMI) application is a Web-based solution that automates documentation of clinical features relevant to each patient's condition and the associated clinical services provided as part of VHA's medical benefits package. The NUMI application retrieves data directly from VA source systems, eliminating redundancy and errors from re-entering patient records and information.

NUMI provides a mechanism by which utilization review can document and record utilization review information within the system. The system then permits physician advisors to re-examine the reviews performed, and then to finalize the review documents. The system permits users to extract reports about patient utilization within the VA system.

NUMI integrates the InterQual Criteria from Care Enhanced Review Management Enterprise (CERMe),

a Commercial-Off-The-Shelf (COTS) product, with Utilization Management (UM) functionality to provide patients with the appropriate level of care. It also integrates with VistA, which permits tight coupling between the patient management systems implemented within the VA and the utilization review function.

To support the Secretary's vision for creating a 21st century VA and to achieve the CIOs five main priorities of improving customer service, managing projects to an outcome, providing operational metrics, ensuring information protection and improving financial reporting, the Office of Information and Technology (OI&T) has undergone a period of review and assessment. Designated positions within OI&T are reorganized and the resulting organizational readjustments for Service Delivery and Engineering, Enterprise Operations (EO) are now in place:
- Data Center Operations (DCO)
- Enterprise Telecommunications (ETM)
- Enterprise Infrastructure Support (EIS)
- EIS Windows
- EIS Mainframe
- EIS UNIX
- EIS Database
- Enterprise Application support (EAS)

There are 23 Veterans Integrated Services Networks (VISNs), providing centralized IT support to 168 medical centers. NUMI will be utilized at all VISNs, to ensure a standard way of capturing and evaluating patient conditions at all the VA facilities. The NUMI application is centrally located at the Austin Information Technology Center (ITC) with the Hines ITC in Illinois as the alternate site in the event of a system failure. The expected number of individuals that will have their PII stored in the system is 800,000.

Completion of this PIA will not result in circumstances that require changes to business processes or result in technology changes.

The System of Record Notice (SORN) 79VA10, "Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

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)

Other data elements here.
Admission date
Admission source
Admitting physician
Discharge date
Attending physician
Current Medications
Previous Medical Records
Facility Treating Specialty
Attending Physician
Service Section
Ward Location
IQ subset
Recommended level of care
Current level of care
Criteria reason

Patient Age
Medical criteria met
Unscheduled 30 day readmit
Comments
Insurance Company Description
Not Met Comment
Medical subset description

PII Mapping of Components

National Utilization Management Integration (NUMI) consists of five key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by National Utilization Management Integration (NUMI) 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
NUMI (Production)	Yes	Yes	• Patient full name • Social Security Number • Admission Dates • Discharge Dates	Patient Care	Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS)
NUMI (Pre-Prod) & NUMI_PS (Product Support)	Yes	Yes	• Patient full name • Social Security Number • Admission Dates • Discharge Dates	Reporting	Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS) and SQL server reporting services

					(SSRS)
NUMI (Reporting Database)	**No**	**No**	• **Patient name** • **Social Security Number** • **Gender** • **Attending Physician** • **Admission Source** • **Admitting Physician**	**Patient Care**	**Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS)**
NUMI Exchange	**Yes**	**Yes**	• **Social Security Number**	**Provides Patient status Updates.**	**Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS)**
NUMI Webservers	**No**	**Yes**	• **Patient full name** • **Social Security Number (last4)** • **Admission Dates** • **Discharge Dates**	**Patient Care**	**Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS)**

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.

PII and PHI are pulled from VistA into the business application NUMI where the data is used to drive workflow related to Utilization Management (UM), which includes the process of ensuring that patients are receiving the right level of care. In order for a NUMI user to have access to PII

through NUMI, the user must have access to VistA. Access to the NUMI software is obtained by authenticating into VistA. Utilization Management information gathered in NUMI is then relayed to VHA Support Service Center (VSSC) for analysis and reporting. VSSC does not receive any PII from NUMI that it does not already get from other sources such as the CDW (Corporate Data Warehouse); however, for the purpose of relating NUMI data back to other patient information in the CDW, PII is transmitted to VSSC. Information is also made available to the national Bed Management System (BMS) used at all VA hospitals. The information is made available through a NUMI Web service interface.

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.

Patient PHI/PII is collected automatically via electronic transmission, using the VistA Interface Adapter (VIA) product to communicate with each instance of VistA.

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.

The information is not checked for accuracy. The NUMI system assumes that VistA information is correct. However, there are various management reports available which would make accuracy issues visible to UM reviewers and managers.

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

System of Records Notice (SORN) 79VA10, "Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.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:
The risk would be the potential exposure patient-level medical PHI/PII to unauthorized users.

Mitigation:
The NUMI system uses the VistA security login system to provide access control. A NUMI user must have patient level VistA access before they can be given access to NUMI. The user connects to NUMI using their PIV/PIN. This ensures that all NUMI users are authorized to access patient-level PHI/PII.

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.

- **Name:** Used to identify the Veteran who is being reviewed.
- **Social Security Number**: Used to verify the identity of the Veteran who is being reviewed.
- Integration Control Number (ICN)
- **Gender:** Used to identify parts of the medical criteria that might apply.

The following fields are all PHI used to manage patient workflow:

- **Facility Treating Specialty**
- **Attending Physician**
- **Service Section**
- **Ward Location**
- **IQ subset**
- **Recommended level of care**
- **Current level of care**
- **Criteria reason**
- **Patient Age**
- **Medical criteria met**
- **Unscheduled 30 day readmit**
- **Comments**
- **Insurance Company Description**
- **Not Met Comment**
- **Medical subset description**
- **Admission source**
- **Admitting physician**
- **Current Medications**
- **Previous Medical Records**

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

The NUMI system provides various reports used by UM reviewers and managers in order to manage patient flow. The reports range in detail from daily patient status to aggregate over time at the ward, facility, and VISN level. The raw patient-level data is made available via Web service to other VHA applications that require parts of the information such as the national Bed Management System. In addition, the raw data is made available to VSSC for use in a UM data cube that provides national UM management information.

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?
The data is encrypted at rest. Data in transit is encrypted by certificates.

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?

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with PIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite e, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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

The data is encrypted at rest. Data in transit is encrypted by certificates.

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.

Access to the PII is determined based on Vista credentials. All clinical staff with patient vista access are eligible for a NUMi account. They must have both NUMi and VistA patient data for one or more facilities There are criteria, procedures, controls, and responsibilities regarding access documented in the form of User and system annual VDL (Virtual Document Library), and there are clinical reports of users by facility by permission. Access does require manager approval. PII Access changes are tracked via logs. The responsible parties for assuring safeguards for the PII are VA employees per system access agreement or VA National Rules of Behavior. All employees and contractors are required go through training every year.

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

Name: Veteran's identification
Social Security Number: Used to verify Veteran identity
Integration Control Number (ICN)
Gender

Current Medications: Used to record current health and medical conditions of the Veterans such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Previous Medical Records: Used to record the history of health and medical conditions of the Veterans such as: Health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Facility Treating Specialty
Attending Physician
Service Section
Ward Location
IQ subset
Recommended level of care
Current level of care
Criteria reason
Patient Age
Medical criteria met
Unscheduled 30 day readmit
Comments
Insurance Company Description
Not Met Comment
Medical subset description
Admission source
Admitting physician

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.

The Veteran's record is to be maintained indefinitely. NARA guidelines as stated in RCS 10-1 records retention schedule. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual.

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.

System of Record Notice (SORN) 79VA10, states: General Records Schedule approved 5.2 item 20 by NARA https://www.archives.gov/files/records-mgmt/grs/grs05-2.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

Data is not removed from NUM.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Directive 6500 VA Cybersecurity Program.

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

NUM staff does not use production data for testing purposes, PII data is protected. NUM does not offer lesser protection for data as PII in all environments and/or networks as well as all applications are treated the same and fully protected.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:
As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

Mitigation:

To mitigate the risk posed by information retention, NUMI adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Schedule 5.2 item 20.

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***
VHA Bed Management Solution (BMS)	Patient records and information	Patient Care Status, SiteID	Secured Web Service
VHA Support Service Center (VSSC)	VSSC provides aggregate reporting for all VHA	Full Replicated Database: All Data elements listed in section 1.1	SQL Server Replication
VistA	Obtain patient information	Name Social Security Number Gender	VIA Interface

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 risk that data contained in the Virtual VA may be shared with unauthorized individuals or that an authorized individual may share it with other unauthorized individuals

Mitigation: NUMI data is only available to personnel with VistA patient access.

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	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: There is a risk that data contained internally may be shared with unauthorized individuals or that those individuals, even when permit to access the data, may share it further with other individuals. The system does not share information with external organizations.

Mitigation: NUMI does not share and or disclose data externally. Protection of sensitive information being transmitted to the NUM system is covered under the Privacy Act and HIPAA regulations. Additionally, username and password are required for access. The principle of need-to-know is strictly adhered to by NUM personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the 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 does provide public notice that the system does exist. This notice is provided in 3 ways:

1) Privacy Act statements are part of all VHA Notice of Privacy Practices which are sent out every 3 years. IB 10-163 Notice of Privacy Practices, https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf, which may be used to submit requests for help.

2) The System of Record Notice (SORN) 79VA10, "Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
3) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA 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."

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

No opportunity or right to decline to provide information is provided by NUM. No information is collected from the Veteran by NUM. Any opportunity or notice of the right to decline to provide information given to the veteran would be given by the source systems that collect the information from the veteran and feed NUM with information.

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

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for VA compensation and pension benefits proceeding. The Privacy Act and VA

policy require that personally identifiable information (PII) only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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 members of the public may not know that the system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record 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.

Individuals wishing to obtain information contained in the NUM system should contact NUM staff or the Department of Veteran Affairs Privacy Office for guidance on where to submit a written request for the information.

VA National Center for Patient Safety (10E2E)
24 Frank Lloyd Wright Drive
Suite M 2100
PO Box 486
Ann Arbor, MI 48106-0486
Email: NCPS@va.gov
Phone: 734-930-5890

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.

The procedure for correcting inaccurate or erroneous information begins with an individual requesting the records in question from the record as described in section 7.1 The individual then submits a written request for the information to be amended. The request for amendment and correction is sent to a VHA Privacy Officer for processing. The amendment request may need to be forwarded to a VHA facility Privacy Officer at a facility where the individual was treated to update the information in VISTA at that location.

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.

Veterans and other Individuals are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP), IB 10-163, https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf, which states:

Right to Request Amendment of Health Information

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
• File an appeal
• File a "Statement of Disagreement"
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

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.

VA Chief Privacy Officer (CPO) in conjunction with VA Privacy Service provide individuals the ability to have inaccurate Personally Identifiable Information (PII) maintained by the organization corrected or amended by publishing Privacy Act regulations and rules (e.g., Directives and Handbooks), which govern how individuals may request that their records maintained in a Privacy Act system of records be amended or corrected. They also review and transmit Privacy Act requests to the appropriate Administration or Staff Office PO or Freedom of Information Act/Privacy Officer (FOIA/PO) for processing.

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: There is a risk that an individual may accidentally provide incorrect information in his correspondence.

Mitigation: Veterans provide information at the local VA Medical Center. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

System/server access is granted by ePAS. Application access is granted by facility clinical management via user role

OIT documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training; and retains

individual training records for 7 years. This documentation and monitoring is performed using Talent Management System (TMS).

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?

Yes. VA contractors have access to the system and PII. They obtain access via ePas approval requests. This access is required for Development and Sustainment activities.

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.

OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter.

Yes. VA contractors have access to the system and PII. They obtain access via ePas approval requests. This access is required for Development and Sustainment activities

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the

end of the training session.

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

If Yes, provide:

1. *The Security Plan Status,* current
2. *The Security Plan Status Date,* (07-Jun-2021)
3. *The Authorization Status,* - current
4. *The Authorization Date,* 02-Nov-2020
5. *The Authorization Termination Date,* (02-Nov-2023)
6. *The Risk Review Completion Date,* (15-Sep-2021)
7. *The FIPS 199 classification of the system* (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.***

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.

No.

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.

N/A

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

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).

The System does not use Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.08.23 14:14:13 -07'00'

Privacy Officer, Phillip Cauthers

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2022.08.29 12:45:36 -04'00'

Information System Security Officer, Joseph Facciolli

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2022.08.24 06:31:42 -04'00'

Information System Owner, Jeffrey Rabinowitz

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).

System of Record Notice (SORN) 79VA10, "Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf**.**

VA Notice of Privacy Practices (NOPP) IB 10-163: https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf