Privacy Impact Assessment for the VA IT System called:

Resident Assessment Instrument/Minimum Data Set

Veterans Health Administration (VHA)

OIT, SPM, Health Service Portfolio, Patient Care Services & VHA 12GEC Geriatrics and Extended Care

Date PIA submitted for review:

March 30, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Neil Cruz	Neil.Cruz@va.gov	(202)632-7422
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	484-432-6161

Abstract

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

The Resident Assessment Instrument/Minimum Data Set (RAI/MDS) is utilized to assess residents of long-term care facilities, guide the development of individualized care plans, evaluate the quality of care provided, identify quality measures as well as capture resident preferences for care, determine workload and determine allowable reimbursements.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Minimum Data Set (MDS) – VASI ID #1571, OIT, Software Product Management (SPM) Health Service Portfolio, Patient Care Services

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

A repository of the standardized patient assessments for VHA's Community Living Centers (CLCs) and State Veterans Homes' nursing homes. The standardized assessments, which are referred to as MDS by health care associates are completed in applications external to the Minimum Data Set Repository (1571), per Centers for Medicare and Medicaid (CMS) requirements for the SVHs and VHA's recommendations for CLCs. These assessments are then uploaded by the repository users via the MDS repository website. The MDS repository is then used to perform comprehensive reporting and to allow comparative review of care.

C. Indicate the ownership or control of the IT system or project.

Resident Assessment Instrument/Minimum Data Set-VA-Owned and VA Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The VA Community Living Centers (CLC) and State Veterans Homes (SVH) system currently contains more than 3.5 million assessment records.

E. A general description of the information in the IT system and the purpose for collecting this information.

A repository of the standardized patient assessments for VHA's Community Living Centers (CLCs) and State Veterans Homes' nursing homes. The standardized assessments, which are referred

to as MDS by health care associates are completed in applications external to the Minimum Data Set Repository (VASI ID #1571), per Centers for Medicare and Medicaid (CMS) requirements for the SVHs and VHA's recommendations for CLCs. These assessments are then uploaded by the repository users via the MDS repository website. The MDS repository is then used to perform comprehensive reporting and to allow comparative review of care.

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

The MDS system consists of a database server and two webservers. One webserver is for internal VA users and the other is an external public facing webserver. Each of the webservers allow either a Community Living Center (CLC) or a State Veteran Homes (SVH) to upload their facility MDS report. The webservers also allow users to run reports (facility, region, and enterprise) according to their role. The VA's Caribou software (VASI ID #2290) is a data feeder to MDS by transmitting MDS Resident Assessment Instruments batch files from all VA CLC's. The VA's Veterans Equitable Resource Allocation (VERA) (VASI ID #1737) is a data consumer from MDS to VERA for certain staffing and financial data.

G. 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.

The MDS system is physically located in the Austin Information Technology Center (AITC) in Austin Tx. PII and PHI and other VA sensitive data is stored persistently within MDS according to VA and NARA data retention laws, regulations and policies. The system is secured according to all Federal and VA laws, regulation and policies, including VA Directive 6500 and the NIST 800-53 Risk Management Framework and Continuous Monitoring series. The internal webserver is 2 Factor Authentication compliant utilizing VA IAM SSOi PIV Card login, and the external public facing webserver is Username/Password for authentication and authorization.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Title 38, United States Code, Section 501.Omnibus Budget Reconciliation Act of 1987, Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA'87). SORN from the OPRM site. 121VA10A7/83 FR 6094 National Patient Databases-VA Federal Register / Vol. 83, No. 29 / Monday, February 12, 2018 / Notices https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

System is not being modified. The system is not in the Cloud. A SORN does exist, but the SORN may need to be revised due to the discovery of an issue with comingling of civilian (non-Veteran PII PHI) uploaded to MDS by the SVH during transmission of the MDS batch file.

D. System Changes

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

The completion of this PIA may result in enablement of 2FA for the external public facing webserver and the elimination of civilian non-Veteran PII/PHI data.

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

The completion of this PIA may result in enablement of 2FA using VA IAM SSOe (or some other VA approved MFA) for the external public facing webserver and the elimination of civilian non-Veteran PII/PHI data through an automated or manual process.

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 Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number

☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Marital Status
Occupation
Medicare/Medicaid Number
ICD-9/10 codes
Admit Reason
Admission Date
Patient Ward Location
Room Number
Bed number
Treating Specialty
Death Date

PII Mapping of Components (Servers/Database)

Resident Assessment Instrument Minimum Data Set (MDS) consists of 3 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Resident Assessment Instrument Minimum Data Set (MDS) and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
VistA VERA Caribou	Yes Yes Yes	Yes Yes Yes	Name Social Security Date of Birth number Gender Race/ Ethnicity Marital Status Occupation	A repository of the standardized patient assessments for VHA's Community Living Centers (CLCs) and State Veterans Homes'	Resident data viewing, including SSNs, is limited to only those that work

			Medicare/Medicaid Number **ICD-9/10 codes** **Admit Reason** **Admission Date** **Patient Ward Location** **Room Number** **Bed number** **Treating Specialty** **Death Date**	**nursing homes. The standardized assessments, which are referred to as MDS by health care associates are completed in applications external to the Minimum Data Set Repository, per Centers for Medicare and Medicaid (CMS) requirements for the SVHs and VHA's recommendations for CLCs. These assessments are then uploaded by the repository users via the MDS repository website. The MDS repository is then used to perform comprehensive reporting and to allow comparative review of care**	**with those individuals at the facility or otherwise have mission need, e.g., approved research requests, VACO support.**

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The individuals providing the RAI/MDS are the CLC Facility Directors and staff using the CLCRAI (Caribou) VASI ID 2270 and the SVH Facility Directors and staff using a multitude of COTS products as part of the CMS mandated nursing home resident care process.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

MDS imports/receives, and aggregates data exported (batch files) from CLCRAI Caribou software (VASI ID 2270) and from contracted SVH nursing home COTS software. VHA GEC users then use this MDS data to enhance patient care, monitor improvement, prevent avoidable decline whenever possible, and obtain objective data for quality assurance and other studies. MDS utilizes a core set of screening and data elements known as the Minimum Data Set (MDS) for a comprehensive assessment of the patient. Assessments are conducted, and data collected on admission, quarterly, and annually for changes in patient condition. MDS information is a requirement in the Veterans Affairs (VA) Community Living Centers (CLC), the State Veterans Home program, and for all VA-contracted nursing home care as part of their Centers for Medicare and Medicaid (CMS) certification. MDS provides the following benefits: Assist in coordination and provision of patient care; Facilitate meeting the requirements of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Quality Indicator Standards; Provide a system-wide Long-Term Care database; Allow comparison of characteristics and outcomes of VA CLC patients with their civilian community counterparts and with veterans receiving nursing home care in the State Veterans Home program; Allow comparative review of care funded for veterans in non-VA facilities.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

MDS creates the following reports: Changes in Skin Integrity Post-Acute Care, percentage of residents who received the influenza vaccination during the most recent influenza season, residents who received the pneumococcal vaccine during the 12-month reporting period, residents who are receiving an antipsychotic medication during the target period, percentage of short-stay residents who were discharged from the nursing home that gained more independence in transfer, locomotion, and walking during their episodes of care, the percentage of long-stay residents who have experienced one or more falls with major injury reported in the target period or look-back period, percentage of long-stay, high-risk residents with Stage II-IV or unstageable pressure ulcers, percentage of long stay residents who have a urinary tract infection (UTI), percentage of long-stay residents who frequently lose control of their bowel or bladder, percentage of residents who have had an indwelling catheter in the last 7 days, percentage of residents who have had an indwelling catheter in the last 7 days, percentage of long-stay nursing facility residents who are physically restrained on a daily basis, percentage of long-stay residents whose need for help with late-loss Activities of Daily Living (ADLs) has increased when compared to the prior assessment, percentage of long-stay residents who had a weight loss who were not on a physician prescribed weight-loss regimen noted in an MDS assessment during the selected quarter, percentage of long-stay residents who have had symptoms of depression during the 2-week period preceding the MDS 3.0 target assessment date, percentage of long-stay residents who have had a fall during their episode of care, percentage of long-stay residents who are receiving antianxiety medications or hypnotics but do not have evidence of psychotic or related conditions, percentage of long-stay residents who have behavior symptoms, percentage of long-stay residents who experienced a decline in independence of locomotion during the target period, prevalence of antianxiety or hypnotic medication use during the target period, and Resource Utilization Group Scores (RUG) reports.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information contained in MDS is collected directly from the Veteran and or from the provider completing the Resident Assessment Instrument.

1.3b 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.

All data contained in MDS is collected using an Automated Information System (AIS). VA CLC's use Caribou and SVH's use a multitude of COTS products. MDS source data is collected by secure electronic data transfer received from Caribou and other COTS products as a batch file. According to the Centers for Medicare & Medicaid Services', Long-Term Care Facility Resident Assessment Instrument (RAI) User's Manual, October 2019 – Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. (Note: The RAI mandated by OBRA is exempt from this requirement.) The valid OMB control number for the Medicare Prospective Payment System SNF and Swing Bed information collection is 0938-1140 and forms have been approved through January 30, 2020.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

A pre-defined set of resident data fields will populate the RAI MDS software via the Inbound ADT interface (the VistA Link). On the MDS side of the application, the RAI MDS software includes edit and error checking to ensure the data entered on the MDS and subsequently submitted to the Austin Information and Technology Center (AITC) is accurate at the time of submission.

1.4b 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.

MDS does not check for accuracy by accessing a commercial aggregator of information.

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

Omnibus Budget Reconciliation Act of 1987, Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA '87).Title 38, United States Code, Section 501.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: MDS collects Personally Identifiable Information (PII) and other highly sensitive Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information

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 patient during an assessment and in other forms of communication-internal/external
• Social Security Number - Used as a patient identifier and as a resource for verifying income information with the Social Security Administration -internal/external
• Date of Birth - Used to identify age and confirm patient identity- statistical reporting-internal/external
• Gender: Assists in correct identification- statistical reporting- internal/external
• Race/ Ethnicity - Provides demographic race/ethnicity specific health trend identification-statistical reporting-internal/external
• Mailing Address - used to correspond with next of kin/record patient' s last known address-internal/external
• Zip Code - part of mailing address - statistical reporting-internal/external
• Phone Number(s)- used to correspond with patient/next of kin-internal/external
• Email Address - used to correspond with patient/next of kin-internal/external
• Emergency Contact - used to correspond with next of kin - internal/external
• Health Insurance Beneficiary Numbers - used for billing and benefits -internal/external
• Marital Status - Allows understanding of the formal relationship the resident has and can be important for care and discharge planning- statistical reporting-internal/external
• Occupation - helps staffs personalize interactions with the resident and are helpful for care planning purposes-internal/external
• Medicare/Medicaid Number - Assists in correct resident identification and billing-internal/external• ICD-9/10 codes - supplements active diagnoses if not listed on the form- statistical reporting-internal/external
• Admit Reason - assists with care planning-internal/external
• Religion - assists staff in understanding faith based medical decisions and providing religious services while in the nursing home-internal/external
• Admission Date - document the date of admission into the nursing home- statistical reporting-internal/external
• Patient Ward Location - required for delivering medications and meals-internal/external
• Room Number - required for delivering medications and meals-internal/external
• Bed Number - required for delivering medications and meals-internal/external
• Treating Specialty - identifies the general category of services provided- statistical reporting-internal/external
• Death Date - used to identify the day the resident died- statistical reporting-internal/external

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

MDS conduct analysis of the data within the DB to produce reports such as: Percent of High-Risk Residents with Pressure Ulcers
Percent of Low Risk Residents Who Lose Control of Their Bowels or Bladder
Percent of Residents Assessed and Appropriately Given the Pneumococcal Vaccine
Percent of Residents Assessed and Appropriately Given the Seasonal Influenza Vaccine
Percent of Residents Experiencing One or More Falls with Major Injury
Percent of Residents Who Did Not Receive, Due to Medical Contraindication, the Pneumococcal Vaccine
Percent of Residents Who Did Not Receive, Due to Medical Contraindication, the Seasonal Influenza Vaccine
Percent of Residents Who Have Behavior Symptoms Affecting Others
Percent of Residents Who Have Depressive Symptoms
Percent of Residents Who Have Had a Fall
Percent of Residents Who Have/Had a Catheter Inserted and Left in Their Bladder
Percent of Residents Who Lose Too Much Weight
Percent of Residents Who Newly Received an Antipsychotic Medication
Percent of Residents Who Received an Antipsychotic Medication
Percent of Residents Who Received the Pneumococcal Vaccine
Percent of Residents Who Received the Seasonal Influenza Vaccine
Percent of Residents Who Used Antianxiety or Hypnotic Medication
Percent of residents who used Antianxiety or Hypnotic Medication without a Psychotic or Related Condition
Percent of Residents Who Were Assessed and Appropriately Given the Seasonal Influenza Vaccine
Percent of Residents Who Were Offered and Declined the Pneumococcal Vaccine
Percent of Residents Who Were Offered and Declined the Seasonal Influenza Vaccine
Percent of Residents Who Were Physically Restrained
Percent of Residents Whose Ability to Move Independently Worsened
Percent of Residents Whose Need for Help with Activities of Daily Living Has Increased
Percent of Residents with a Urinary Tract Infection
Percentage of Residents Who Made Improvements in Function
As an example – the CMS produced document - "Skilled Nursing Facility Quality Reporting Program Measure Calculations and Reporting User's Manual Version 3.0" page 36 contains one of many very complex analytical calculations available within the MDS system that is run as a report against the MDS DB and contained data:
"Calculating Resident-level Expected QM Scores" For quality measures that use logistic regression in the risk adjustment, a resident-level logistic regression model is estimated. The resident-level observed quality measure score is the dependent variable. The predictor

variables are one or more resident-level covariates associated with the quality measure. Calculation of the quality measure and covariate scores are described in Section 6.2 (Step 5) of this chapter. Each logistic regression had the following form:[1] $QM\ triggered\ (yes{=}1,no{=}0){=}\beta0{+}\beta1{*}COV1{+}\beta2{*}COV2{+}\cdots{+}\beta N{*}COVN$Where:• $\boldsymbol{\beta 0}$ = the logistic regression constant• $\boldsymbol{\beta 1}$= the logistic regression coefficient for the first covariate• $\boldsymbol{COV1}$ = the resident-level score for the first covariate• $\boldsymbol{\beta 2}$= the logistic regression coefficient for the second covariate, where applicable• $\boldsymbol{COV2}$ = the resident-level score for the second covariate, where applicable• $\boldsymbol{\beta N}$= the logistic regression coefficient for the Nth covariate, where applicable• $\boldsymbol{COVN}$ = the resident-level score for the Nth covariate, where applicable• *Note, "N" represents the total number of covariates in the model. Each resident's expected QM score could then be calculated with the following formula:[2] $Resident\ level\ expected\ QM\ score{=}1/[1{+}e{-}x]$Where:• e = the base of natural logarithms• x = a linear combination of the constant and the logistic regression coefficients times the covariate scores (from Formula [1], above). Note: A covariate score will be equal to [1] if the covariate criterion is met for that resident, and equal to [0] if the criterion is not met. As an example, consider the actual calculation used for the expected score for the measure Percent of Residents or Patients with Pressure Ulcers That Are New or Worsened (NQF #0678) (S002.02). The covariates for that QM are obtained from the PPS 5-Day assessment (A0310B = [01] and are the following:• Indicator of requiring limited or more assistance in bed mobility self-performance• Indicator of bowel incontinence at least occasionally• Have diabetes or peripheral vascular disease or peripheral arterial disease• Indicator of Low Body Mass Index, based on Height and Weight The equation used for this example (with the parameters from Table A-221) is:[3] QM$Score{=}1/[1{+}e{-}(\beta0{+}\beta1{*}bedmob{+}\beta2{*}bowel{+}\beta3{*}diabetes{+}\beta4{*}BMI)]$Where:• $\boldsymbol{\beta 0}$ = the logistic regression constant• $\boldsymbol{\beta 1}$= the logistic regression coefficient for bed mobility• Bedmob = the resident-level covariate indicating the need for limited or more assistance in bed mobility• $\boldsymbol{\beta 2}$= the logistic regression coefficient for bowel incontinence at least occasionally• bowel = the resident-level covariate indicating bowel incontinence at least occasionally• $\boldsymbol{\beta 3}$= the logistic regression coefficient for diabetes or peripheral vascular disease or peripheral arterial disease• diabetes = the resident-level covariate indicating diabetes or peripheral vascular disease or peripheral arterial disease• $\boldsymbol{\beta 4}$= the logistic regression coefficient for low body mass index• BMI = the resident-level covariate indicating low body mass index. The values for the covariate parameter for each of the k risk-adjustment coefficients (βk) used for calculating the resident-level expected quality measure scores are presented in Table A-2 and Table A-3 of Appendix A and the associated Risk-Adjustment Appendix File.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The information created by the MDS system is not for any one specific individual (Veteran nursing home resident) but instead the information is for the specific Population of Veteran nursing home Residents. The information and data created by the MDS system is not written back nor stored in any single Veteran nursing home Resident's individual patient record. The information and data

created by MDS is used by authorized Government employees (VISN and VHA GEC National Program Office staff) to make determinations about the VA's CLC and SVH nursing home population.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

All data in transit and at rest are protected by the security controls for the MDS application that cover approximately 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

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

All SSNs are protected by the security controls for the MDS application that cover approximately 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3 , VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

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

All PII/PHI are safeguarded IAW OMB Memo M-06-15 by the security controls for the MDS application cover approximately 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit

and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The security controls for the MDS application cover approximately 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

Every authorized user is responsible for safeguarding PII.

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• Social Security• Date of Birth• Gender• Race/ Ethnicity• Mailing Address• Zip Code• Phone Number(s)• Email Address• Emergency Contact Information• Health Insurance Beneficiary Numbers• Marital Status• Occupation• Medicare/Medicaid Number• ICD-9/10 codes• Admit Reason• Religion• Admission Date• Patient Ward Location• Room Number• Bed number• Treating Specialty• Death Date

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The records are disposed of in accordance with General Records Schedule 5.2 item 20. Item 20 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, SORN 121VA10P2 states: General Records Schedule approved 5.2 item 20 by NARA
https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

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

SORN 121VA10P2 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 or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

"**Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.** https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

RAI MDS does not use any live or real data in the development or testing environments.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by MDS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, MDS 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***
VISTA "CLCRAI/Caribou "VERA	Caribou uses data from VistA. The MDS Web app, is logged into and used to select the created batch file and upload to the MDS Oracle Database. MDS receives data to assess residents of long-term care facilities, guide the development of individualized care plans, evaluate the quality of care provided, identify quality measures as well as capture resident preferences for care, determine workload and determine allowable reimbursements.	•Name •Social Security •Date of Birth •Gender •Race/ Ethnicity •Mailing Address •Zip Code •Phone Number(s) •Email Address •Emergency Contact Information •Health Insurance Beneficiary Numbers •Marital Status •Occupation •Medicare/Medicaid Number •ICD-9/10 codes •Admit Reason •Religion •Admission Date •Patient Ward Location •Room Number •Bed number •Treating Specialty •Death Date	MDS Web app, is logged into and used to select the created batch file and upload it to the MDS Oracle Database through secure electronic data transfer.

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*

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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***
State Veteran Homes	For the creation and completion of the Minimum Data Set (MDS) 3.0, and the Care Area Assessments	•Name •Social Security •Date of Birth •Gender •Race/ Ethnicity •Mailing Address •Zip Code •Phone Number(s) •Email Address •Emergency Contact Information •Health Insurance Beneficiary Numbers •Marital Status •Occupation •Medicare/Medicaid Number •ICD-9/10 codes •Admit Reason •Religion	SORN121VA10P2 https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm Routine uses 1-5. Title 38, United States Code, Section 501. Omnibus Budget Reconciliation Act of 1987, Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA '87).	MDS Web app, is logged into and used to select the created batch file and upload it to the MDS Oracle Database through secure electronic data transfer. VA CLC Users use PIV Cards to login. SVH Users use Username/Password to login.

		•Admission Date •Patient Ward Location •Room Number •Bed Number •Treating Specialty •Death Date		

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 FIPS 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, or transmitted between IT centers.
4. Internal protection is managed by access controls such as two factor authentication (2FA), user IDs and passwords, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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: . The privacy risk associated with sharing VA sensitive data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Additionally, there is a privacy threat of a breech during the transmission of the data

Mitigation: Protection of sensitive information being transmitted to the MDS system is covered under the Privacy Act and HIPAA regulations. Additionally, two factor authentication (2FA) Personal Identity Verification (PIV) Cards for CLC, and for SVH username and password are required for access. The principle of need-to-know is strictly adhered to by MDS 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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

MDS receives data from the VHA VISTA system. VHA is required to send out the VHA Notice of Privacy Practices every 3 years. The VHA notice specifically addresses how VHA will use and disclose health information. The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways: 1) The System of Record Notice (SORN) 121VA10P2 https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm 2)
This Privacy Impact Assessment (PIA) also serves as notice of the MDS system. As required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(l)(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."

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

Please see attached for most current notice.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

MDS receives data from the VHA VISTA system. VHA is required to send out the VHA Notice of Privacy Practices every 3 years. The VHA notice specifically addresses how VHA will use and disclose health information. The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways: 1) The System of Record Notice (SORN) 121VA10P2 https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm 2)

This Privacy Impact Assessment (PIA) also serves as notice of the MDS system. As required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(l)(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.

VHA Directive 1605.1 "Privacy and Release of Information" lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

VHA Handbook 1605.1 "Privacy and Release Information" lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 MDS application 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?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to obtain more information about access, redress and record correction of MDS system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10P2. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

MDS is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

MDS is a Privacy Act system which does conform to the Privacy Act and is included in the active published SORN mentioned throughout this PIA document.

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.

Individuals wishing to obtain more information about access, redress and record correction of MDS system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10P2. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm

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.

Individuals wishing to obtain more information about access, redress and record correction of MDS system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10P2. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2014-02-11/html/2014-02890.htm

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress is provided via the SORN.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the data within the MDS system. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about application.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Per VA Directive and Handbook 6300, 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.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

RAI/MDS users are vetted through the VA 9957 process and user accounts are established via the Customer User Provisioning System (CUPS). State Home users log on using application-specific authentication locally managed at the AITC. Once logged on, the user can transmit MDS batch records and can access existing RAI/MDS reports according to the privileges assigned to the role of the user. At this time all users are assigned the same privileges. The VA 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 through the use of VA's Talent Management System (TMS).

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

RAI/MDS users are vetted through the VA 9957 process and user accounts are established via the Customer User Provisioning System (CUPS). State Home users log on using application-specific authentication locally managed at the AITC. Once logged on, the user can transmit MDS batch records and can access existing RAI/MDS reports according to the privileges assigned to the role of the user. At this time all users are assigned the same privileges.

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.

VA contract employee access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Additionally, contractors are required to sign a Business Associate Agreement (BAA).

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 prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security awareness training which all personnel must complete via the VA's Talent Management System (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 is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS

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

8.4a If Yes, provide:

1. *The Security Plan Status:Active*
2. *The System Security Plan Status Date:* 10/12/2022
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* Minimum Data Set 02/04/2022
5. *The Authorization Termination Date:* Minimum Data Set ATD 01/20/2024
6. *The Risk Review Completion Date:* 12/08/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

No, RAI MDS does not utilize cloud technology. The system is located in the VA's Austin Information Technology Center (AITC) on government owned government operated (GOGO) communications and computing infrastructure (C&CI).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of*

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

Not applicable.

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.

Not applicable.

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.

Not applicable.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

Not applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.04.17 15:57:39 -04'00'

Privacy Officer, Dennis Lahl

Neil F. Cruz 341838 Digitally signed by Neil F. Cruz 341838
Date: 2023.04.18 07:47:37 -04'00'

Information Systems Security Officer, Neil Cruz

Temperance M. Leister 3514567 Digitally signed by Temperance M. Leister 3514567
Date: 2023.04.19 11:42:59 -05'00'

Information Systems Owner, Temperance Leister

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).

121VA10A7/83 FR 6094 National Patient Databases-VA Federal Register / Vol. 83, No. 29 / Monday, February 12, 2018 / Notices

https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

VHA Notice of Privacy Practices

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices