Privacy Impact Assessment for the VA IT System called:

Homeless Management Information Systems

Veterans Health Administration (VHA)

Mental Health Services

eMASS ID #31

Date PIA submitted for review:

5/09/2024

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)	James Alden	james.alden@va.gov	781-687-2768
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?".

Homeless Management Information System (HMI) is a software application designed to record and store client-level information on the characteristics and service needs of homeless persons. An HMI is typically a web-based software application that homeless assistance providers use to coordinate care, manage their operations, and better serve their clients. HMI implementation presents communities with an opportunity to re-examine how homeless services are provided in their community, and to make informed decisions, and develop appropriate action steps. Because the implementation of HMI systems varies from community to community, examples of local implementation covering the community planning process, software selection and implementation are available from a variety of communities.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

Homeless Management Information Systems is owned by the owned by the Veterans Health Administration (VHA) Homeless Programs Office . It is one component of a larger project to create a VA Registry of homeless Veterans. The VA HMI Repository is essentially a gateway for sending data. It collects data exported from HMI applications around the country, validates it, processes it into a structural dataset, and transfers it to a different application called the VA Homeless Registry (which is a component of the Analytics and Business Intelligence LAN) where data analysis and reporting occur. HMI does this by providing a secure web-based interface that allows users to upload a zipped file containing data that they have extracted from their HMI applications, either in the HUD HMI Comma Separated Value (CSV) or HUD HMI Extensible Markup Language (XML) formats. The VA HMI Repository transfers data to the VA Homeless Registry (ABI LAN) via a batch process that runs every 24 hours. This batch process is a one-way data bridge that allows HMI to upload data to the VA Homeless Registry for future analysis and reporting.

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

HMI is a comprehensive repository (data warehouse) of information about homeless Veterans who receive services provided by VA administered programs.

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

Owned by the Veterans Health Administration (VHA) Homeless Programs

2. *Information Collection and Sharing*

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

The system stores 10,000+ individuals within the HMI database and is comprised of Veterans at risk of homelessness.

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

Homeless Management Information System (HMI) is a software application designed to record and store client-level information on the characteristics and service needs of homeless persons.

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

The VA's Homeless Management Information Systems (HMI) application, owned by the Veterans Health Administration (VHA) Homeless Programs Office, is one component of a larger project to create a VA Registry of homeless Veterans. The VA's HMI is comprehensive repository (data warehouse) of information about homeless Veterans who receive services provided by VA administered programs. The repository is essentially a gateway for sending data.

G. *Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

Homeless Management Information Systems (HMI) is currently hosted hybrid at the Philadelphia Information Technology Center (PITC) and in the Azure Government Cloud (Virginia) and is managed by the Web Operations (WebOps) team which is part of the Enterprise Web Infrastructure Support (WEBOPS) organization.

3. Legal Authority and SORN

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

Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986. Public Law 110-387, Veterans' Mental Health and Other Care Improvements Act of 2008.

The information collected by this system falls under SORN 121VA10, "National Patient Databases-VA". https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501

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?*

Yes, the SORN does cover it.

The SORN does not need to be modified or updated at this time.

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

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

Other PII/PHI data elements:
Health Insurance
Veteran Status
Disabling Condition
Residence Prior to Program Entry
Length of stay in Previous Place
Zip Code of Last Permanent Address
Housing Status
Program Entry Date
Program Exit Date
Unique Person Identification Number
Household Identification Number
Source and Amount of Income
Income Received in Last 30 Days
Non-Cash Benefits
Non-Case Benefits Received in Last 30 Days
Destination
Financial Assistance Provided
Housing Relocation & Stabilization Services Provided
Veteran's Information
Category of Permanent Housing
Formerly Chronically Homeless
Currently Chronically Homeless
Percent of Area Median Income (AMI)

PII Mapping of Components (Servers/Database)

Homeless Management Information Systems consists of **one** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Homeless Management Information Systems** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program	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

Interface (API) etc.) that contains PII/PHI					
Database Server #1	Yes	Yes	Name, date of birth, SSN, address, phone numbers, service and benefits information, as well as medical data. Name, Social Security Number, Data of Birth, Mother's Maiden Name, Mailing Address, Zip Code, Phone Number(s), Email Address, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Race, Ethnicity, Gender, Veteran Status, Disabling Condition, Residence Prior to Program Entry, Length of stay in Previous Place, Zip Code of Last Permanent Address, Housing Status, Program Entry Date, Program Exit Date, Unique Person Identification Number, Household Identification Number, Source and Amount of Income, Income Received- in Last 30 Days, Non-Cash Benefits Received in Last 30 Days, Destination, Financial Assistance Provided, Housing Relocation & Stabilization Services Provided, Veteran's Information, Category of Permanent Housing, Formerly Chronically Homeless, Currently	Identification of homeless Veterans; reach out to Veterans and communicate benefits; provide homeless Veterans access to health care.	Database is encrypted

			Chronically Homeless, Percent of AMI.		

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?

Supportive Services for Veteran Families (SSVF) grantees enter client-level data into HMI applications across the country. The VA HMI Repository provides a secure web interface that allows that data collected by SSVFs to be uploaded to the repository and transferred to the VA Homeless Registry for further analysis and reporting.

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.

Supportive Services for Veteran Families (SSVF) grantees enter client-level data into HMI applications across the country. The VA HMI Repository provides a secure web interface that allows that data collected by SSVFs to be uploaded to the repository and transferred to the VA Homeless Registry for further analysis and reporting.

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

Supportive Services for Veteran Families (SSVF) grantees enter client-level data into HMI applications across the country. The VA HMI Repository provides a secure web interface that allows that data collected by SSVFs to be uploaded to the repository and transferred to the VA Homeless Registry for further analysis and reporting.

1.3 How is the information collected?

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

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

The HMI Repository does not collect data directly from the Veterans. HMI receives secure electronic file transfers. There is no direct interconnection, however, Supportive Services for Veteran Families grantees using Department of Housing and Urban Development Homeless Management Information Systems located at Continuums of Care across the country upload files exported from their local HMI to the VA HMI via a web interface.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

The HMI Repository does not collect data directly from the Veterans. HMI receives secure electronic file transfers. There is no direct interconnection, however, Supportive Services for Veteran Families grantees using Department of Housing and Urban Development Homeless Management Information Systems located at Continuums of Care across the country upload files exported from their local HMI to the VA HMI via a web interface.

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.

HMI provides system messages and email notifications to end users and admins for the success or failure of the file uploaded. A dataset may be determined to be unusable if data quality is too low (e.g., there are clients with program entry dates that precede their program exit dates) and rejected altogether. The system provides the ability for administrative users to modify thresholds on a per-program basis and provides an overwrite warning when a file is uploaded into the system for a program that already contains an upload for the current month.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

N/A

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

Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986.
Public Law 110-387, Veterans' Mental Health and Other Care Improvements Act of 2008.

The information collected by this system falls under SORN 121VA10, "National Patient Databases-VA". https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.
Authority for maintenance of the system: 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: HMI collects Personally Identifiable Information (PII) and other highly delicate 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 aid 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 can better protect the individual's information. The local administrator provides approved and authorized users their access to HMI. Furthermore, users of VA sensitive information complete a security awareness training on at least an annual basis.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

HMI Repository business benefits include the following capabilities:

- Define the inventory of agencies from which the VA programs are operated.
- Define Supportive Services for Veteran Families SSVF, Grant and Per Diem (GPD), and Health Care for Homeless Veterans (HCHV) programs from which data will come and match them to the program definition.
- Allow for the import of data from SSVF, GPD, and HCHV grantees and contractors HMI applications into the Repository. All of these programs will use non-VA, locally run HMI to enter data which is then uploaded into the VA HMI Repository.
- Provide the ability to check data quality by comparing counts at different times, checking for capacity utilizations, and checking for missing responses.
- Reduces the overall data management burden by staff that are processing the data.
- Provide the ability to transfer data to the VA Homeless Registry, and possibly other data systems.
- Provide the ability to upload data sets compliant with current HUD data standards.
- Support federal policy mandates to develop local Coordinated Entry Systems that are often dependent on the collection of HMI data. The capacity of the Repository to collect information from SSVF, GPD, and HCHV allows VA to encourage VA funded community providers to support federal policies and track their compliance with this mandate.
- Provide the ability to determine whether an individual is a Veteran eligible for services in real-time, avoiding the delays inherent in the traditional process of establishing eligibility. This can have a critical impact on the health and welfare of homeless Veterans who are at high risk for emergent health and mental health as delays in accessing care may result in serious health consequences.
- Uses:
  - *Name - Veteran's identification*
  - *Social Security Number-used to verify Veteran identity and as a file number*
  - *Date of Birth- Veteran's identification*
  - *Mother's Maiden Name- Veteran's identification*
  - *Mailing Address -Used to correspond with the Veteran*
  - *Zip Code - Used to correspond with the Veteran – statistical reporting*
  - *Phone Number(s) -Used to correspond with the Veteran*
  - *Email Address -Used to correspond with the Veteran*
  - *Health Insurance– used to support Veteran's benefits eligibility*

- *Current Medications -Assist front-line caregivers in care giving and case management – statistical reporting*
- *Previous Medical Records -Assist front-line caregivers in care giving and case management– statistical reporting*
- *Race – statistical reporting*
- *Ethnicity – statistical reporting*
- *Gender – statistical reporting – support relocation to shelter*
- *Veteran Status – statistical reporting – support benefits, eligibility*
- *Disabling Condition-Assist front-line caregivers in care giving and case management– statistical reporting*
- *Residence Prior to Program Entry – statistical reporting– support relocation to shelter*
- *Length of stay in Previous Place– statistical reporting– support relocation to shelter– support benefits, eligibility*
- *Zip Code of Last Permanent Address– statistical reporting– support relocation to shelter– support benefits, eligibility*
- *Housing Status– statistical reporting– support relocation to shelter– support benefits, eligibility*
- *Program Entry Date– statistical reporting– support benefits, eligibility*
- *Program Exit Date– statistical reporting– support benefits, eligibility*
- *Unique Person Identification Number -Veteran's identification –case management*
- *Household Identification Number–case management*
- *Source and Amount of Income– support benefits, eligibility – statistical reporting*
- *Income Received in Last 30 Days– support benefits, eligibility – statistical reporting*
- *Non-Cash Benefits – support benefits, eligibility – statistical reporting*
- *Non-Cash Benefits Received in Last 30 Days– support benefits, eligibility – statistical*
- *reporting*
- *Destination– support benefits, eligibility – statistical reporting*
- *Financial Assistance Provided– support benefits, eligibility – statistical reporting*
- *Housing Relocation & Stabilization Services Provided– support benefits, eligibility – statistical reporting*
- *Veteran's Information– support benefits, eligibility – statistical reporting*
- *Category of Permanent Housing– support benefits, eligibility – statistical reporting*
- *Formerly Chronically Homeless– support benefits, eligibility – statistical reporting*
- *Currently Chronically Homeless– support benefits, eligibility – statistical reporting*
- *Percent of AMI– support benefits, eligibility – statistical reporting*

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

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

The VA HMI Repository provides a secure web interface that allows for data collected by SSVFs to be uploaded to the repository and transferred to the VA Homeless Registry for further analysis and reporting. No analysis is done by the HMI Repository.

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 VA HMI Repository provides a secure web interface that allows for data collected by SSVFs to be uploaded to the repository and transferred to the VA Homeless Registry for further analysis and reporting. No analysis is done by the HMI Repository.

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?

Secure electronic file transfer. Both HMI Repository and the VA Homeless Registry (ABI LAN) are applications hosted by Infrastructure Operations (IO)

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

Secure electronic file transfer. Both HMI Repository and the VA Homeless Registry (ABI LAN) are applications hosted by Infrastructure Operations (IO)

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

Secure electronic file transfer. Both HMI Repository and the VA Homeless Registry (ABI LAN) are applications hosted by Infrastructure Operations (IO)

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access is determined by the user's role and the Facility Implant Coordinator

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

The types of controls that are in place for HMI are as follows: The minimum-security requirements for HMI a high impact system cover security/privacy related 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/privacy related 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, Authority and Purpose (AP), Accountability, Audit, and Risk Management (AR), Data Quality and Integrity (DI), Data Minimization and Retention (DM), Individual Participation and Redress (IP), Security (SE), Transparency (TR), Use Limitation (UL). Our facilities employ all security/privacy controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 Rev 4 and specific VA directives

2.4c Does access require manager approval?

Role based access limits the scope and access the users have to information in HMI.

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

Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior. Additionally, HMI users must also take VA HIPPA focused training and VA Privacy and Information Security Awareness training before gaining access to HMI system both are required to be taken on an annual basis. Role based access limits the scope and access the users have to information in HMI

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

Every VA employee is responsible for protecting PII however the ultimate responsibility for an IT system falls upon the Information System Owner regarding safeguarding IT system data.

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 Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Email Address
- Health Insurance
- Current Medications
- Previous Medical Records
- Race
- Ethnicity
- Gender
- Veteran Status
- Disabling Condition
- Residence Prior to Program Entry
- Length of stay in Previous Place
- Zip Code of Last Permanent Address
- Housing Status
- Program Entry Date
- Program Exit Date
- Unique Person Identification Number
- Household Identification Number
- Source and Amount of Income
- Income Received in Last 30 Days
- Non-Cash Benefits
- Non-Cash Benefits Received in Last 30 Days

- Destination
- Financial Assistance Provided
- Housing Relocation & Stabilization Services Provided
- Veteran's Information
- Category of Permanent Housing
- Formerly Chronically Homeless
- Currently Chronically Homeless
- Percent of AMI

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 retained and disposed of in accordance with General Record Schedules (GRS) 5.2 020. GRS 5.2 020 disposition instructions are to destroy upon verification of successful creation of the final document or file, or wen no longer needed for business use, whichever is later.

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

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

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

The records are disposed of in accordance with GRS 5.2 020. The GRS can be located at https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf.

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

The records are disposed of in accordance with GRS 5.2 020 and disposition authority DAA-GRS-2022-0009-0002. The GRS can be located at 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 media sanitization, when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with VA 6500 and NIST 800-53 Rev 4.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

HMI resides on a production, pre-production, and development environment. The production environment handles PHI/PII data; preproduction is used for staging the application after new releases/changes and before deploying to production; access to the development environment is strictly limited to the application developers. The HMI program follows the guidance provided by the Veteran Focused Integration Process (VIP), and agreed upon requirements are worked and tested before the application is released to production. User testing may also take place as part of a new version release, depending on the extent of the changes. In addition, VHA programs may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA Directive 6511.

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 HMI 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, HMI adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in Records Schedule in accordance with VA media destruction policies.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Homeless Registry (a component of the Analytics and Business Intelligence LAN, ABI LAN) Which is owned by the Analytics and Business Intelligence Program	Data uploaded to the HMI Repository is transferred to the VA Homeless Registry for analysis and reporting	Name Social Security Number Date of Birth Mother's Maiden Name Mailing Address Zip Code Phone Number(s) Email Address Health Insurance Beneficiary Numbers Current Medications Previous Medical Records Race Ethnicity Gender, Veteran Status Disabling Condition Residence Prior to Program Entry Length of stay in Previous Place Zip Code of Last Permanent Address Housing Status Program Entry Date Program Exit Date Unique Person Identification Number Household Identification Number Source and Amount of Income Received in Last 30 Days Non-Cash Benefits Non-Cash Benefits	Secure electronic file transfer. Both HMI Repository and the VA Homeless Registry (ABI LAN) are applications hosted by Infrastructure Operations (IO)

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*
		Received in Last 30 Days Destination Financial Assistance Provided Housing Relocation & Stabilization Services Provided Veteran's Information Category of Permanent Housing Formerly Chronically Homeless Currently Chronically Homeless Percent of AMI	

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: There is a risk that data transferred in the HMI may be shared with unauthorized VA individuals or that authorized individuals may share it with other unauthorized individuals.

Mitigation: Access control procedures mitigate the chance of unauthorized users. Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training. In order to access HMI data authorized users are required to authenticate through the use of Multi-Authentication with their Personal Identity Verification PIV card and pin.

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 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

*If no External Sharing listed on the table above, **(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> There is limited risk for external sharing of data contained in the HMI system.

<u>Mitigation:</u> Currently, there is a not an authorized permanent external connection to the HMI system. All data access is authorized through the VA.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

The System of Record Notice (SORN) 121VA10 - National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice of the HMI 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."

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

N/A

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.

The System of Record Notice (SORN) 121VA10 - National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice of the HMI 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
.

.Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. 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.

Not in the HMI system, any right to consent to particular uses of the information would be handled by the source systems that collect the information from the Veteran and are uploaded to the HMI Repository.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

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:

<u>Privacy Risk:</u> There is a risk that members of the public may not know that the HMI system exists within the Department of Veterans Affairs.

<u>Mitigation:</u> 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 with links provided in Appendix A, including the PIA, System of Record Notice, and VA Notice of Privacy Practices.

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 https://department.va.gov/foia// 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 HMI system should contact the Department of Veteran's Affairs as directed in the System of Record Notice (SORN) 121VA10 – National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

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)?

The system is not exempt from 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?

The information is contained in a Privacy Act System of Record.

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.

VHA Directive 1605.1 paragraph 8 states that an individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually-identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR 164.526. The right to seek an amendment of this information or records is a personal right of the individual to whom the record pertains. The personal representative of a deceased individual has a right to request an amendment of the decedent's records.

An amendment request must be in writing, signed, and must adequately describe the specific information the individual believes to be inaccurate (i.e., faulty or not conforming exactly to truth), incomplete (i.e., unfinished or lacking information needed), irrelevant (i.e., inappropriate or not pertaining to the purpose for which records were collected), or untimely (i.e., before the proper time or prematurely) and the reason for this belief.

To correct HMI information, participants should contact the SSVF grantee that provided them services. A list of grantees and contact information is available at www.va.gov/homeless/ssvf.

Individuals wishing to obtain more information about access, redress and record correction of HMI system should contact the Department of Veteran's Affairs as directed in the System of Record Notice (SORN) 121VA10 – "National Patient Databases-VA". This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

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.

To correct HMI information, participants should contact the SSVF grantee that provided them services. A list of grantees and contact information is available at www.va.gov/homeless/ssvf

Also as stated in the written and published SORN as listed above, individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (19F4), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the National Service Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

To correct HMI information, participants should contact the SSVF grantee that provided them services. A list of grantees and contact information is available at www.va.gov/homeless/ssvf

Individuals wishing to obtain more information about access, redress and record correction of HMI system should contact the Department of Veteran's Affairs as directed in the System of Record Notice (SORN) 121VA10 - National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> The individual may not know the relevant procedures for gaining access to, correcting, or contesting their information.

<u>Mitigation:</u> By publishing this PIA and the applicable SORN, the VA makes the public aware of the HMI system. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about this application: individuals may write or call the Director of National Data Systems (19F4), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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 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.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. The documentation and monitoring are performed using the VA Talent Management System (TMS).

Access to HMI is granted by submitting a VA Form 9957 Access Form with appropriate functional task codes to Program staff, who grant system access. System admins receive the 9957 requests, send it to the LDAP group for userID (Account Management) and they send the account information back to the system administrator. Elevated privilege occurs when a user is granted the ability to do more than a standard user. A standard user is someone that has “zero administrative” privileges in any capacity.

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?

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.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. The documentation and monitoring are performed using the VA Talent Management System (TMS).

Access to HMI is granted by submitting a VA Form 9957 Access Form with appropriate functional task codes to Program staff, who grant system access. System admins receive the 9957 requests, send it to the LDAP group for userID (Account Management) and they send the account information back to the system administrator. Elevated privilege occurs when a user is granted the ability to do more than a standard user. A standard user is someone that has “zero administrative” privileges in any capacity.

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.

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.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. The documentation and monitoring are performed using the VA Talent Management System (TMS).

Access to HMI is granted by submitting a VA Form 9957 Access Form with appropriate functional task codes to Program staff, who grant system access. System admins receive the 9957 requests, send it to the LDAP group for userID (Account Management) and they send the account information back to the system administrator. Elevated privilege occurs when a user is granted the ability to do more than a standard user. A standard user is someone that has "zero administrative" privileges in any capacity.

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 the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is 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 the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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 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 privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training (TMS#10203) is required initially and annually thereafter.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 30-Apr-2024
3. *The Authorization Status:* Granted
4. *The Authorization Date:* 29-Jan-2024
5. *The Authorization Termination Date:* 27-Jul-2024
6. *The Risk Review Completion Date:* 12-Jan-2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

N/A

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)*

VA Enterprise Cloud (VAEC) - Information Technology Management as a Service (ITMaaS)

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.*

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).

N/A

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

ID	Privacy Controls
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.05.14 14:59:27 -07'00'

Privacy Officer, Phillip Cauthers

JAMES ALDEN

Digitally signed by JAMES ALDEN
Date: 2024.05.20 15:45:48 -04'00'

Information System Security Officer, James Alden

TEMPERANCE LEISTER

Digitally signed by TEMPERANCE LEISTER
Date: 2024.05.15 11:37:18 -05'00'

Information System 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; screen shot of a website collection privacy notice).

The System of Record Notice (SORN) 121VA10 – "National Patient Databases-VA"
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Directive 1605.04: Notice of Privacy Practices