Privacy Impact Assessment for the VA IT System called:

Health Benefits Management Systems (HBMS)

Veterans Health Administration

VHA Claims & Appeals Modernization Office (CAMO)

eMASS ID # 2567

Date PIA submitted for review:

10/17/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Melvin Davis	Melvin.Davis3@va.gov	504-875-7280
Information System Owner	Kenton Ngo	Kenton.Ngo@va.gov	303-349-6138

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The VHA Health Benefits Management Systems (HBMS) automates the current dental benefit eligibility determination process thereby allowing VA clinical staff to quickly validate Veterans' dental benefits prior to scheduling an appointment. HBMS alleviates the task of having to login to multiple systems. The system extracts eligibility information using automation and internal application programming interfaces (APIs) to integrate with VA Master Person Index (VA MPI) and VA Profile. Once a determination is made, eligibility information is shared with the VA Dental Record Manager Plus (DRM Plus) system using Veterans Data Integration and Federation Enterprise Platform (VDIF-EP) APIs.

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?

Health Benefits Management Systems (HBMS) is owned by VHA Claims and Appeals Modernization Office (CAMO).

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

HBMS automates the current dental benefit eligibility determination process thereby allowing VA clinical staff to quickly validate Veterans' dental benefits prior to scheduling an appointment. HBMS enables staff to access multiple systems to determine patient classification, eligibility, and referrals without having to login to multiple systems.

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

This is a VA Controlled / non-VA Owned and Operated system.

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?

HBMS contains data from benefits-eligible veterans and/or dependents who request dental services. HBMS is expected to store information on approximately 700,000 individuals/annually.

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

HBMS stores Veteran and dependent dental benefit eligibility information. The system allows VA clinical staff to obtain information from internal VA sources to quickly validate Veterans' dental benefits prior to scheduling dental appointments. The information is used to determine patient classification, eligibility, and referrals. Information from the disparate systems will provide staff with the information they can use to determine patient classification, eligibility, and referrals which will ultimately determine dental care eligibility. Once eligibility is determined, classification details will be stored in HBMS using the patients Integrated Control Number (ICN) as an identifier.

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

HBMS shares information with VA Master Person Index (VA MPI), VA Profile, and Veterans Data Integration and Federation Enterprise Platform (VDIF-EP).

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?*

HBMS is used by VA enrollment and eligibility department and dental clinical staff from different physical locations. However, the system is not operated at multiple sites.

3. Legal Authority and SORN

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

Authority for Maintenance of the System: Title 38 U.S.C. §501 and 38 U.S.C. §7304.

HBMS is covered by the following three SORNs:

- 192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA* 2023-23327.pdf (October 23, 2023)
- 121VA10 / 88 FR 22112, *National Patient Databases-VA* 2023-07638.pdf (April 12, 2023)
- 150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA* 2023-24193.pdf (November 12, 2023)

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?*

No, the SORNs do not require amendment or revision. HBMS uses cloud technology (storage) that is covered in existing SORNs.

4. System Changes

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

No business processes will be changed as a result of the completion of this PIA. HBMS is a new tool that will be used to replace the current manual activity performed by administrative staff who must login to multiple systems to determine patient classification, eligibility, and referrals.

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

No, there will not be any technology changes.

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: Benefits Information, Electronic Data Interchange Personal Identifier (EDIPI), Business Email Address

PII Mapping of Components (Servers/Database)

HBMS consists of three key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HBMS 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 Interface (API) etc.) that contains PII/PHI	**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**
Health Benefits Management Systems (HBMS)	Yes	Yes	• Medical Records • Integrated Control Number (ICN) • Military History/Service Connection • Benefits Information • Name (VA Employee/Contractor) • Business Email Address	To identify patients to determine eligibility, and to document eligibility	Use of SSO for access to the system by internal VA users
Health Benefits Management Systems (HBMS)	Yes	No	• Name (Veteran/Dependent) • Full Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Gender/Sex	To identify patients to determine eligibility, and to document eligibility	Use of SSO for access to the system by internal VA users

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
			• Electronic Data Interchange Personal Identifier (EDIPI)		
VA Profile	Yes	Yes	• Medical Records • Military History/Service Connection • Benefits Information	To determine patient eligibility	HTTPS/ Transfer Layer Security (TLS)
VA Master Person Index (VA MPI)	Yes	Yes	• Name (Veteran/Dependent) • Full Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Medical Records • Gender/Sex • Integrated Control Number (ICN) • Electronic Data Interchange Personal Identifier (EDIPI)	To determine patient eligibility & Corresponding Ids	HTTPS/ Transfer Layer Security (TLS)

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?

Identifying information (e.g., name, SSN, DOB) is collected by VA dental facility clinical staff directly from the Veteran or beneficiary. The identifying information is verified against VA MPI and then used to collect additional information from other VA sources (i.e., VA Profile, VA MPI). The eligibility determination for Veterans will be passed back and updated to VistA via VDIF-EP.

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.

HBMS is used to validate benefits. Therefore, patient eligibility information must be obtained and validated from sources other than the individual.

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

No, HBMS does not create information and is not a system of record.

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?

HBMS extracts eligibility information using automation and multiple internal application programming interfaces (APIs) to integrate with VA Master Person Index (VA MPI) and VA Profile. The patient information is initially collected electronically from VA Profile and VA MPI and then analyzed by the application to make a dental eligibility determination. The automated determination is then saved to HBMS and then sent to the patient's VistA record via VDIF-EP.

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?

Information is not collected on a form and is therefore not subject to the Paperwork Reduction Act.

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.

Information received is verified by the system to ensure the Veteran and/or their dependents are eligible and/or authorized to receive the care and that the claim is valid and appropriate. HBMS will match Veterans to the VA MPI based on search of traits or EDIPI lookup when Veterans request information or appointments. VA MPI will maintain the accuracy of the

Veteran identity data and will push any changes to HBMS for processing of the corrections. Because of the nature of dental eligibility, HBMS will calculate the eligibility for the Veteran when the Veteran is touched by the system. When a Veteran record is searched, HBMS will pull the latest information from VA MPI and VA Profile related to the dental eligibility. Dental eligibility will be assessed through a business process automation engine and results will be displayed and logged for auditing. The business process automation engine will be thoroughly tested before implementation of the application and when any new rules are added. Both auditing and review of records will be available. Patient eligibility information will be shared with Veterans Data Integration and Federation Enterprise Platform (VDIF-EP).

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?

Data accuracy is not checked using a commercial aggregator because the data is sourced from internal VA systems (VA Profile and VA MPI).

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The collection of documents within HBMS is governed by 38 U.S.C. 501, 7304 and 38 U.S.C 501.

The SORNs for the system are:

- 192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA* 2023-23327.pdf (October 23, 2023)
- 121VA10 / 88 FR 22112, *National Patient Databases-VA* 2023-07638.pdf (April 12, 2023)
- 150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA* 2023-24193.pdf (November 12, 2023)

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.*

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

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

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

Follow the format below when entering your risk assessment:

<u>Privacy Risk:</u> Due to the sensitive nature of the data, there is a risk that if the data were accessed by an unauthorized individual or otherwise breached, personal or professional harm may result for the individuals affected.

<u>Mitigation:</u> Pega Cloud® uses data-at-rest encryption (DARE) in all Pega Cloud environments. "Data at rest" refers to any content that the cloud service saves on a hard drive. Encryption of data at rest is implemented for all sandbox and production environments. All client data stored in volumes, databases, and S3 buckets in a Pega Cloud environment are encrypted with 256-bit Amazon Web Services (AWS) encryption. The keys are rotated on a regular basis and are securely stored in Amazon Key Management Service (KMS). In addition, while SSNs will be used for locating applicable persons from the Master Veteran index, SSNs will not be relied upon for internal person identification. When visible to the end user, SSNs will be masked to show only last 4.

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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to Search VA MPI	Not used
Full Social Security Number	Used to Search VA MPI	Not used
Date of Birth	Used to Search VA MPI	Not used
Mother's Maiden Name	Used to Search VA MPI	Not used
Personal Mailing Address	Used to Search VA MPI	Not used
Personal Phone Number(s)	Used to Search VA MPI	Not used
Medical Records	Used to determine eligibility	Not used

PII/PHI Data Element	Internal Use	External Use
Gender/Sex	Used to Search VA MPI	Not used
Integrated Control Number	Used as an internal identifier	Not used
Military History/Service Connection	Used to determine eligibility	Not used
Benefits Information	Used to determine eligibility	Not used
EDIPI	Used to Search VA MPI	Not used
Name (Employee/Contractor)	Part of HBMS user profile	Not Used
Business Email Address (Employee/Contractor)	Part of HBMS user profile	Not Used

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 HBMS system compiles data from VA sources to determine eligibility for dental services. The determinations are made by a series of business rules that are predefined by the Office of Dentistry and the department of Enrollment and Eligibility. HBMS will apply the business logic rules engine to determine the eligibility status of the Veterans that are being looked up.

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.

Eligibility determinations are determined using business process automation when VA staff look up the patients' records. Once entered into HBMS, the patients' eligibility is shared with the VA Dental Record Manager Plus (DRM Plus) system using APIs via VDIF-EP to update the corresponding VistA data.

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?

Application security in Pega is configured at three levels:

- Data in transit

- Data at rest
- Data at display

Data in transit is secured with transport-level encryption for browser-based sessions and authentication profiles for connectors and services. Data at rest is secured with an encryption mechanism provided by the database vendors/providers. Pega supports encryption of individual database columns as well. Pega has built-in encryption capability to encrypt data using advanced encrypt standard. Data at the display is secured by defining access control policies based on roles and attributes.

Pega Cloud for Government (PCFG) inherits controls from FedRAMP High controls

Encryption Module	**FIPS 140-2 Certificate #**	**System Component(s)**
AWS Elastic Load Balancer (ELB)	# 4523	• Customer Stack HTTPS and Transport Layer Security (TLS) Connections • Predictive Diagnostic Cloud (PDC) Application HTTPS and TLS Connections
AWS Virtual Private Network (VPN)	# 4523	Customer Stack VPN Connections
AWS Relational Database Service (RDS)	# 4523	• Customer Stack Databases • PDC Application Database
AWS Key Management Service (KMS)	# 4523	Encryption Key Management
AWS Nitro Card Security Engine	# 3739	Data in Transit
AWS S3 Buckets	# 4523	Data at Rest
CheckPoint	# 4264	Remote Access / VPN
Okta IDaaS Certificate	# 4370	Authentication
Okta IDaaS Certificate	# 4370	Digital Signatures/Hash
Secure Kernel Code Integrity-(Windows)	# 3096	Operating System Configuration
Libgcrypt Cryptographic Module-(RedHat Linux)	# 3784	Operating System Configuration

The PCFG system inherits the above encryption functionality and controls from the AWS Infrastructure as a Service (IaaS). The AWS IaaS maintains a FedRAMP Authorized package providing statements describing AWS implemented encryption security controls. Please refer to the AWS FedRAMP Authorized package for details. All of the AWS services within PCFG use cryptographic keys provided by the AWS Key Management Service hardware security module (HSM) (Cryptographic Module Validation Program (CMVP) Certificate # 4523). Recently, the AWS Application Load Balancer (ALB) uses a new certificate for FIPS 140-3 (CMVP Certificate #4631).

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

SSNs are used by the HBMS system to obtain patient identity from VA MPI but will not be used by clinical staff to identify patients. When SSNs are displayed, they will be masked to show only the last 4 digits.

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

Users accessing HBMS must be authenticated during login. Additionally, users that access HBMS must agree to the Privacy Information Security Agreement Rules of Behavior once a year which dictates how VA employees use/safeguard PII/PHI.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

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

All VA employees and contractors are required to go through privacy, information security and VA Rules of Behavior (ROB) training. This training ensures that the end users know how to properly handle PII. Beyond the training, the system is designed to secure the data. Access to PII is granted within the system by System Administrators enabling users to view, modify, add, or remove data based on user roles and responsibilities.

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

All training is documented and tracked through VA Talent Management System (TMS) (https://www.tms.va.gov). Standard Operating Procedures (SOPs) are documented. Additionally, there is a Pega Cloud for Government System Security Plan (SSP).

2.4c Does access require manager approval?

Yes, a ServiceNow work ticket must be submitted by the user's Manager in order to access HBMS.

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

Yes, an audit trail of all patient retrievals are captured in HBMS and can be retrieved or reviewed at a later date.

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

The Information System Security Officer (ISSO) is ultimately responsible for ensuring safeguards for the 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*

The following PII/PHI data elements are retained in the system:

- Integrated Control Number
- Medical Records
- Military History/Service Connection
- Benefits Information
- Name (VA Employee/Contractor)
- Business Email Address

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.*

Records in HBMS are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 4.2 (Information Access and Protection Records) and 5.2, (Transitory and Intermediary Records), item 020, (Intermediary records).

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 retention periods described in Question 3.2 reflect General Records Schedules (GRS) published by the National Archives Records Administration (NARA).

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

The records retention schedule, series and disposition authority are:

- General Records Schedule, 5.2, Transitory and Intermediary Records, item 020, Intermediary records and disposition authority DAA-GRS 2022-0009 0002 https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf
- General Records Schedule, 4.2, Information Access and Protection Records and disposition authority https://www.archives.gov/files/records-mgmt/grs/grs04-2.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 PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. 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.

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.*

Development and testing environments do not allow the use of PII. Therefore, HBMS does not use PII for research, testing, or training.

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: The risk to maintaining data within HBMS is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: HBMS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).

- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
- System access is only granted to authorized VA contractors and clinical staff.
- Electronic storage media used to store, process, or access records is disposed of in adherence with VA Directive 6500 (VA Cybersecurity Program).

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 Profile	Receiving patient information for eligibility determination	• Medical Records • Military History/Service Connection • Benefits Information	Electronic – API- HTTPS/ Transfer Layer Security (TLS)
VA Master Person Index (VA MPI)	Receiving patient information for eligibility determination	• Name • Full Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Medical Records • Gender/Sex • Integrated Control Number (ICN)	Electronic – API- HTTPS/ Transfer Layer Security (TLS)

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***
		• Electronic Data Interchange Personal Identifier (EDIPI)	
Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)	Sharing patient eligibility information	• Medical Records • Integrated Control Number (ICN) • Benefits Information	Electronic – API- HTTPS/ Transfer Layer Security (TLS)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> Privacy Information may be released to unauthorized individuals.

<u>Mitigation:</u> HBMS adheres to information security requirements instituted by the VA Office of Information Technology (OIT). Both VA contractors and VA employees are required to take Privacy, HIPAA, and information security training annually. Additionally, information is shared in accordance with VA Handbook 6500.

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:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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 VHA Notice of Privacy Practice (NOPP) 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 Veterans enrolled for VA health care benefits or eligible to enroll for VA health care benefits regardless of if they are receiving care from VA. Non-Veterans receiving care are provided the notice at the time of their encounter. The NOPP can be downloaded from the following web address: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice 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." The PIA is housed on the VA Privacy Service PIA website: https://department.va.gov/privacy/privacy-impact-assessments/

Notice is also provided in the Federal Register with the publication of the SORNs:

- 192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA* 2023-23327.pdf (October 23, 2023)
- 121VA10 / 88 FR 22112, *National Patient Databases-VA* 2023-07638.pdf (April 12, 2023)
- 150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA* 2023-24193.pdf (November 12, 2023)

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

Notice was provided and can be found here: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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.

Notice is not provided on forms or web sites: The VHA Notice of Privacy Practice (NOPP) is a document which 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 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." The PIA is housed on the VA Privacy Service PIA website: https://department.va.gov/privacy/privacy-impact-assessments/

Notice is also provided in the Federal Register with the publication of the SORNs:

- 192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA* 2023-23327.pdf (October 23, 2023)
- 121VA10 / 88 FR 22112, *National Patient Databases-VA* 2023-07638.pdf (April 12, 2023)
- 150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA* 2023-24193.pdf (November 12, 2023)

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.

Individuals seeking dental services are not obligated to supply information. The information they supply is used to help determine eligibility for dental services. They have a right to decline sharing information which could prevent an eligibility determination.

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.

Individuals cannot consent to particular uses of the information provided. However, individuals can decline to share their information. If individuals do not share their information, eligibility for dental services cannot be determined.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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 Transparency: *Has sufficient notice been provided to the individual?*

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer. The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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.***

First party rights to information are provided through the Privacy Act. For further guidance, please see Record Access Procedures via the system SORNs:

192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA*; Record Access Procedures: Individuals seeking access to records in this system pertaining to them must contact the system manager in writing. The request for access must contain the requester's full name, address, telephone number, and signature, and describe the records sought in sufficient detail to enable VA to locate them with a reasonable amount of effort.

121VA10 / 88 FR 22112, *National Patient Databases-VA*: Record Access Procedures: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address and telephone number, be signed by the requester and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort

150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA*: Record Access Procedures: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above, or write, call or visit the VA facility location where they are or were employed or made contact. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort

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)?

HBMS 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?

HBMS is a Privacy Act system.

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 have the right to request an amendment (correction) to their information if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. Requests must be submitted in writing, specify the information that needs to be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains their information.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans are informed of the amendment process in the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains their information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"

- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

However, individuals may mail or fax requests to: Department of Veterans Affairs, Freedom of Information Act Services (005R1C), 811 Vermont Avenue, NW, Washington, DC 20420, Fax: 202-632-7581.

Additional notice is provided through the SORNs listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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 as outlined in the System of Records Notice. Contesting Record Procedures: Individuals seeking to contest or amend records in this system pertaining to them must contact the system manager in writing as indicated above. A request to contest or amend must state clearly and concisely what record is being contested, the basis for contesting it, and the proposed amendment to the record.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The NOPP, SORN, and this PIA discuss the process for requesting an amendment to one's records. The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.

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?

In accordance with the Enterprise Identity and Demographics Records-VA (150VA10) SORN and locally established data security procedures, access to file information is controlled at two levels. First, the systems recognize authorized employees by a series of individually unique passwords/codes as a part of each data message. Second, the employees are limited to only that information in the file which is needed in the performance of their official duties.

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?

All HBMS users are internal to the agency and the system does not share any information externally. Therefore, other agencies will not have access to HBMS. In accordance with the National Patient Databases-VA (121VA10) SORN, access to and use of national patient databases are limited to those persons whose official duties require such access and VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests.

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.

In accordance with the National Patient Databases-VA (121VA10) SORN and locally established data security procedures, access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access. Server level access is granted to developers on an as needed basis by the Information Security Officer (ISO). The ISO has granted server access to a small set of trusted developers approved to work with and diagnose production issues. Access within the system is granted by System Administrators who enable users to view, modify, add, or remove data based on user roles and responsibilities. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, HBMS contractors will have access to the system. Contractors will also be involved in the design, development, and maintenance of the system. All contractors who will utilize HBMS have signed NDAs.

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.

General Training includes: VA Privacy Rules of Behavior, Privacy awareness training, HIPPA and VA on-boarding enterprise-wide training. Users 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 security awareness training that all personnel must complete via VA’s Talent Management System 2.0 (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 2.0 system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not Yet Approved
2. *The System Security Plan Status Date:* This does not apply to this system
3. *The Authorization Status:* Assess Only
4. *The Authorization Date:* November 18, 2024
5. *The Authorization Termination Date:* November 18, 2025
6. *The Risk Review Completion Date:* This does not apply to this system
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)*

HBMS uses cloud technology. HBMS uses Pega Cloud for Government hosted on AWS Government Cloud. Pega is FedRAMP authorized Platform as a Service (PaaS).

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.*

Yes, there is an agreement in place between the VA and Pega Cloud Service Provider (CSP). VA has full ownership of the PII that will be used by HBMS as outlined in the contract agreement. Contract Name: Pega Platform as a Service (PaaS) & Software as a Service (SaaS) - Contract Number: NNG15SD21B, Order Number: 36C10B24F0369

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.

Ancillary data is not collected by Pega.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, this principle is described in the contract with the cloud provider. The cloud service provider does not collect ancillary data. VA has full authority over data stored in HBMS.

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

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

No robotic process automation (RPA) is used in this system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.12.10 13:33:35 -05'00'

Privacy Officer, Nancy Katz-Johnson

MELVIN DAVIS

Digitally signed by MELVIN DAVIS
Date: 2024.12.10 13:07:52 -06'00'

Information System Security Officer, Melvin Davis

KENTON NGO

Digitally signed by KENTON NGO
Date: 2024.12.10 14:08:39 -07'00'

Information System Owner, Kenton Ngo

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).

NOPP
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORNs

- 192VA30 / 88 FR 72820, *Veterans Affairs Profile-VA* 2023-23327.pdf (October 23, 2023)
- 121VA10 / 88 FR 22112, *National Patient Databases-VA* 2023-07638.pdf (April 12, 2023)
- 150VA10 / 88 FR 75387, *Enterprise Identity and Demographics Records-VA* 2023-24193.pdf (November 12, 2023)

VA Privacy Service PIAs:

https://department.va.gov/privacy/privacy-impact-assessments/

VA Privacy, Policies, and Legal Information

https://www.va.gov/privacy-policy/

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 Handbook 1605.04: Notice of Privacy Practices 1605.04