Privacy Impact Assessment for the VA IT System called:

Bed Management Solution (BMS)

(EPMO)Veterans Health Administration

OI&T Enterprise Program Management Office

eMASS ID #11

Date PIA submitted for review:

11-3-2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katzjohnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	John Hale	John.Hale4@va.gov	859-233-4511x3517
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

Bed Management Solution (BMS) is a real-time, user-friendly, web-based Veterans Health Information Systems and Technology Architecture (VistA) interface for tracking patient movement, bed status, and bed availability. BMS allows administrative and clinical staff to record, manage, and report on the planning, patient movement, patient occupancy, and other activities related to management of beds. All patient admission, discharge, and transfer movements are sent directly from VistA to BMS.

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?

Bed Management Solution (BMS), (EPMO)Veterans Health Administration

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

Bed Management Solution (BMS) is a real-time, user-friendly, web-based Veterans Health Information Systems and Technology Architecture (VistA) interface for tracking patient movement, bed status, and bed availability. BMS allows administrative and clinical staff to record, manage, and report on the planning, patient movement, patient occupancy, and other activities related to management of beds. All patient admission, discharge, and transfer movements are sent directly from VistA to BMS.

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

VA Owned and VA Operated IS

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?

There are currently over 25 million distinct veteran patient records in the BMS database dating back to 1992. Included in that information are Patient name, SSN, and Date of Birth. Records for deceased patients are part of those records. There are currently between 2500 and 400 concurrent end users of BMS. Both figures are expected to increase over time.

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

The data in BMS is being collected from the existing VistA files and patient requests in person or online at the VAMCs. The clinical medical staffs enter the patient information into BMS using Application for Health Care Benefits (Form 1010EZ).

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

BMS shares information with National Utilization Management Integration (NUMI), Veterans Data Integration and Federation (VDIF), Emergency Department Integration Software (EDIS) and Cerner through Veterans Data Integration and Federation (VDIF) through the BMS background processors.

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?*

Only BMS users who require access designated by certain roles can obtain access to PII in BMS. Access is managed and maintained by site administrators. BMS maintains logs of user activity, which could track recent and historical access to PII. The BMS Application is utilized across 144 VAMC facilities.

3. Legal Authority and SORN

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

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register (Vol. 85, No. 192) for publication electronically as an official document of the Department of Veterans Affairs. James P. Gfrerer, Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on June 16, 2020 for publication. Title 38, United States Code, Sections 501(b) and 304. Notice is provided by the system's System of Record Notice (SORN), Patient Medical Records 24VA10A7 that covers Veteran / dependent health information.

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

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)

Other PII/PHI data elements: Add Additional Information Collected: Patient sex, health condition, and admitting diagnosis, Room Bed, Ward Location, Admission, Discharge, Transfer (ADT), Specialty, Treating Specialty, Facility Movement Type, Order able Item, Medical Center Division, Patients Pending

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

Bed Placement List, Disposition Date Time, Patient IEN, Facility Code, Complaint, Diagnosis Date Time, Level of Care, Review Date.)

PII Mapping of Components (Servers/Database)

Bed Management Solution consists of **22** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Bed Management Solution** 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
BMS Primary Production Database Used by Production Application	Yes	Yes	• Name • Social Security Number • Date of Birth • Patient sex • Health condition • Admitting diagnosis • Personal Mailing Address • Hospital Location, • Room Bed, • Ward Location, • Admission, Discharge, Transfer (ADT), • Specialty, • Treating Specialty,	BMS collects PII because … "[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, patient movement, patient occupancy, and bed availability. It also provides performance information that can be used to improve patient flow within, and between, VA	Internally (Primary Databases) Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

			• Facility Movement Type, • Order able Item, • Medical Center Division, • Patients Pending Bed Placement List • Disposition Date Time • Patient IEN • Facility Code • Complaint • Diagnosis Date Time • Level of Care • Review Date	**Medical Centers (VAMCs).**	
BMS_REPL **Primary replicated database (1 of 2) Used for Primary Reporting**	**Yes**	**No**	**• Name • Social Security Number • Date of Birth • Patient sex • Health condition • Admitting diagnosis • Personal Mailing Address • Hospital Location, • Room Bed, • Ward Location, • Admission, Discharge,**	PII because … “[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, patient movement, patient occupancy, and bed availability. It also provides performance information that can be used to	Internally (Primary Databases) Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

			Transfer (ADT), **• Specialty,** **• Treating Specialty,** **• Facility Movement Type,** **• Order able Item,** **• Medical Center Division,** **• Patients Pending Bed Placement List** **• Disposition Date Time** **• Patient IEN** **• Facility Code** **• Complaint** **• Diagnosis Date Time** **• Level of Care** **• Review Date**	improve patient flow within, and between, VA Medical Centers (VAMCs).	
BMS_REPL **Primary Replicated database (2 of 2) Used for Health Systems Reporting**	**Yes**	**Yes**	**• Name** **• Social Security Number** **• Date of Birth** **• Patient sex** **• Health condition** **• Admitting diagnosis** **• Personal Mailing Address** **• Hospital Location,**	PII because … "[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, patient movement, patient occupancy, and bed availability. It	Internally (Primary Databases Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

			• Room Bed, **• Ward Location,** **• Admission, Discharge, Transfer (ADT),** **• Specialty,** **• Treating Specialty,** **• Facility Movement Type,** **• Order able Item,** **• Medical Center Division,** **• Patients Pending Bed Placement List** **• Disposition Date Time** **• Patient IEN** **• Facility Code** **• Complaint** **• Diagnosis Date Time** **• Level of Care** **• Review Date**	also provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs).	
BMS Primary Pre-Production database	**Yes**	**Yes**	**• Name** **• Social Security Number** **• Date of Birth** **• Patient sex** **• Health condition** **• Admitting diagnosis**	PII because … "[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, patient	Internally (Primary Databases) Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness

			• Personal Mailing Address **• Hospital Location,** **• Room Bed,** **• Ward Location,** **• Admission, Discharge, Transfer (ADT),** **• Specialty,** **• Treating Specialty,** **• Facility Movement Type,** **• Order able Item,** **• Medical Center Division,** **• Patients Pending Bed Placement List** **• Disposition Date Time** **• Patient IEN** **• Facility Code** **• Complaint** **• Diagnosis Date Time** **• Level of Care** **• Review Date**	movement, patient occupancy, and bed availability. It also provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs).	and required reporting of suspicious activity.
BMS_REPL Pre-Production Replicated database (1/2)	**Yes**	**Yes**	**• Name** **• Social Security Number** **• Date of Birth**	PII because … “[to] provide [a] real time, web-based system for VA clinical staffs	Internally (Primary Databases) Safeguards implemented to ensure data is not sent to the wrong

Used for BMS Reporting			**• Patient sex** **• Health condition** **• Admitting diagnosis** **• Personal Mailing Address** **• Hospital Location,** **• Room Bed,** **• Ward Location,** **• Admission, Discharge, Transfer (ADT),** **• Specialty,** **• Treating Specialty,** **• Facility Movement Type,** **• Order able Item,** **• Medical Center Division,** **• Patients Pending Bed Placement List** **• Disposition Date Time** **• Patient IEN** **• Facility Code** **• Complaint** **• Diagnosis Date Time** **• Level of Care** **• Review Date**	to record, manage, and report on the planning, patient movement, patient occupancy, and bed availability. It also provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs).	VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

BMS_REPL Pre-Production Replicated Database (2/2) Used for Health Systems Reporting	**Yes**	**Yes**	**• Name • Social Security Number • Date of Birth • Patient sex • Health condition • Admitting diagnosis • Personal Mailing Address • Hospital Location, • Room Bed, • Ward Location, • Admission, Discharge, Transfer (ADT), • Specialty, • Treating Specialty, • Facility Movement Type, • Order able Item, • Medical Center Division, • Patients Pending Bed Placement List • Disposition Date Time • Patient IEN • Facility Code • Complaint**	PII because … "[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, patient movement, patient occupancy, and bed availability. It also provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs).	Internally (Primary Databases) Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

			• Diagnosis Date Time • Level of Care • Review Date		

1.2 What are the sources of the information in the system?

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

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

The data source in BMS is being collected from the existing VistA files and patient requests in person or online at the VAMCs. The information is stored to the local and national BMS Data Warehouse databases.

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.

VHA takes reasonable steps to confirm the accuracy and relevance of the PII and PHI it collects. VHA tries to collect PII directly from the individual whenever possible, which allows for better confirmation of the accuracy, relevant, timeliness and completeness of the information. If information is collected in person verbally or on a VA form this confirmation happens as part of the process. When information is collected online or through the mail, confirmation of PII is handled through other processes, such as computer matches. VHA collects PII from the individual whenever possible. There are processes in place and a hierarchy for collecting information from others when an individual, such as a patient, is unable to provide the needed PII. When PII is collected from a person other than the individual to whom it pertains this is usually notated.

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

The BMS application provides various reports containing metrics that assist with patient flow, planning, and review. These reports are all provided from the BMS_REPL (replicated) database. Additionally, there are reports provided by the Health Systems team that extract report data from the additional BMS_REPL to provide to those users.

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 information BMS stores is primarily collected from the source of record, VistA. Other updates, however, such as icon assignments, bed statuses, and bed cleaning actions are entered via the end user or mapped automatically by the system's many workflows.

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?

BMS does not subject to 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.

All PII and PHI is reviewed for accuracy as it is collected and utilized to care for Veterans. Any PII or PHI identified or determined to be inaccurate or outdated, or erroneously placed in the wrong record by VHA staff is updated administratively immediately as appropriate. VHA will also update any PII in a Privacy Act system of records pursuant to a granted amendment request from the individual. VHA Directive 1605.01 outlines policy for processing amendment requests. Other policies, such as VHA Directive 1907.01 outlines how health records are updated including administratively due to errors.

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?

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

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

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

BMS system contains a Consolidated Health Record (CHR) for patients and includes identifying information such as Social Security Number, medical history, employment history, medical benefit and eligibility information, and patient admission and discharge information. The Authority provided under the SORN 24VA10A7 is Title 38, United States Code, Sections 501(b) and 304.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

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

Follow the format below when entering your risk assessment:

<u>Privacy Risk:</u> The BMS collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

<u>Mitigation:</u> The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of facility common security controls. These issues are identified and described in the system security plans for the individual information systems.

The BMS system uses PIV/PIN to provide access control. A BMS user must have certain roles before they can be given access to BMS. The user connects to BMS using their PIV/PIN login credentials. This ensures that all BMS users are authorized to access patient-level PHI/PII.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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 identify patient in a bed and/or transferred to/from beds across VA facilities	N/A
Social Security Number (SSN):	Used to uniquely identify a bed patient	N/A
Date Of Birth (DOB):	Used to determine bed patient age.	N/A
Mailing Address:	Used to identify bed patient mailing address.	N/A
ZIP:	Used to identify bed patient mailing address zip code.	N/A
Ward Occupancy/Location:	Used to provide list of bed assignments, records patient's movement and notifies that bed is assigned to a patient.	N/A
Bed grouping:	Used to view a group of beds assigned within a unit.	N/A
Scheduled admission:	Used to determine scheduled admissions, anticipated discharges, available beds, closed beds, isolation, flight risk patients or SI patients, restrained patients, gender, patient's length of stay, bed status tracking, bed availability, ready for cleaning, and beds in use.	N/A
Integrated sites:	Used to understand integrated medical center facility and sites.	N/A
Patient waiting for bed:	Used as a Yes/No indicator to show # of patients waiting for beds.	N/A
Reports:	Various reports on patient movement, performance of bed management, facility site reports.	N/A
Patient Sex:	Used to determine patient's gender	N/A

Health Condition:	Used to store last known overall patient status	N/A
Admitting Diagnosis:	Diagnosis entered upon admission of patient	N/A
Hospital Location:	The patient may be discharged from a VAMC, but needs additional care at a location such as continuing care facility (e.g. PHARMACY, OPTHAMOLOGY, IMAGING). BMS treats this a Discharge Clinic.	N/A
Room Bed:	Patient's current Room/Bed location within a hospital location. Note that rooms can have multiple or single beds.	N/A
Admission, Discharge, Transfer (ADT):	**Admission** - the patient is admitted to the hospital/medical center. **Discharge** - the patient is discharged (exit/release) from the hospital/medical center. **Transfer** - the patient is physically moved to another area, usually a different ward or facility.	N/A
Specialty:	The type of therapy that the Room/Bed/Ward typically provides, e.g. REHAB, ORTHOPEDIC, PSYCHIATRY, etc..	N/A
Treating Specialty:	The general type of therapy that a patient will undergo, e.g. ORTHOPEDIC, VASCULAR, NEUROLOGY, etc.. (In relation to their diagnosis)	N/A
Facility Movement Type:	The type of movement that can happen within a facility, facilities can choose their own movement types.	N/A
Order Able Item:	Orderable Items are individual requests that transmit from VistA with their own IENs that typically are actions/needed items for the patient, such as "ACETAMENOPHIN TAB" or "DISCHARGE". These are not unique to the patient, but	N/A

	unique across other orderable items.	
Medical Center Division:	A VAMC can have multiple divisions (or alternate locations, satellite sites). E.g. V23OMA has Des Moines, Iowa City, Omaha)	N/A
Patients Pending Bed Placement List:	Also referred to as a Waiting List, this list exists at the Regional, VISN and Facility level. Patients on this list transferred, admitted, or discharged. This list of patients are awaiting a bed admission, generally.	N/A
Disposition Date Time:	The timestamp (date and time) of the patient's latest disposition during their stay in the medical center. Most commonly, BMS has been used for EDIS for date to be admitted.	N/A
Patient IEN:	Used to uniquely identify a patient within a VistaSite. IEN=Internal Entry Number. Note that a Patient IEN will be different across Vista sites.	N/A
Facility Code:	A Three letter abbreviation of a facility name or location. E.g. Michael Debakey/Houston = "HOU"	N/A
Complaint:	Also known as the Presenting Problem, this is the patient's (or patient's caretaker) reason for being at the hospital	N/A
Level of Care:	Evaluation of whether the patient's care is being met, per the NUMI integration.	N/A
Review Date:	The timestamp (date and time) of the patient's latest review of file and status, per the NUMI Integration	N/A

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?

A BMS does not analyze or produce patient data. The system is designed to provide bed status and bed availability for Veterans when they are being admitted into the VAMCs for medical care. Various reports on patient movement, performance of bed management, facility site reports, etc.

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.

BMS does not create or make available new or previously unutilized information about an individual.

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?

BMS has encryption compliant and meets the VA6500 requirements for data at rest encryption as well as data in transit.

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

The full patient SSN is masked/hidden throughout the BMS application and reporting either by only displaying the last 4 digits of the SSN or masking the first 5 digits, e.g.XXX-XX-1234.

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

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

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:

<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?

Only BMS users who require access designated by certain roles can obtain access to PII in BMS. Access is managed and maintained by site administrators. BMS maintains logs of user activity, which could track recent and historical access to PII.

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

Yes

2.4c Does access require manager approval?

Yes

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

VA Network Authentication, along with BMS Authorization controls, are used to restrict access to appropriate personnel. Access is monitored, tracked, and logged.

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

All BMS staff are responsible for protecting PII and the use of proper procedures pertaining to safe handling and prevention of inappropriate distribution of PII.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security Number, Date of Birth, Patient sex, Health condition and Admitting diagnosis.

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.*

In accordance with the SORN and the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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?

In accordance with the SORN and the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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

In accordance with the SORN and the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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.

Under the jurisdiction of VHA, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov. VA

Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.

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.

All IT system and application development and deployment are handled by VA OI&T. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA 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 policy. As referred in the 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 BMS 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, the BMS adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

A toll-free phone number will be established for data breach incidents potentially involving a large (500+) number of individuals. When one occurs the number is activated and posted, along with a Health Information Technology for Economic and Clinical Health (HITECH) Press Release, on the VA Notices web page: http://www.va.gov/about_va/va_notices.asp.

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***
National Utilization Management Integration (NUMI)	National Utilization Management Integration (NUMI)	Service • Call<Inpatient>(PII/PHI/SPI) ○ Admission ID ○ SSN ○ Level of Care ○ Review Date	VDIF
Veterans Data Integration and Federation (VDIF)	VDIF	• Name • Social Security Number • Date of Birth • Patient sex • Health condition • Admitting diagnosis	VDIF
Cerner	Cerner	• Hospital Location, • Patient, • Room Bed, • Ward Location, • ADT, • Specialty, • Treating Specialty, • Facility Movement Type, • Order able Item, • Medical Center Division, • Patients Pending Bed Placement List	VDIF
Emergency Department Integration Software (EDIS)	EDIS	• Disposition Date Time • Patient IEN • Facility Code • Complaint • Diagnosis Date Time	VDIF

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:

Privacy Risk: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

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

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
No External System				

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> N/A

<u>Mitigation:</u> N/A

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)
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 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."

Notice is also provided in the Federal Register with the publication of the SORN: SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

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.

Notice is also provided in the Federal Register with the publication of the SORN: SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their right to consent to uses of their information. The Notice states “To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.”

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:

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 BMS prior to providing the information to the BMS.

Mitigation: Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) 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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) Office. VHA Directive 1605.01, Privacy and Release of Information, outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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)?

BMS 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?

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

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 are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

A Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations whom had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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 risk of incorrect information in an individual's records is mitigated by authenticating information when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses 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.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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?

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS). Access to the system is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. Each user role in BMS is identified by the Roles Definition folder created in the system.

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?

There are no users from other agencies outside of the VA that will have access to BMS.

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.

Primary users (write group): The group allows members to add patients waiting for a bed, puts beds out of service, makes additions to the ward white board. Primary Environment Management Users (EMS): The EMS write group allows EMS to edit and update the bed cleaning process but not to the other parts of the bed board. Membership in this group does not give access to the regular BMS home page. Primary and Secondary Clinical Users (Read only group): allows staff to look at web pages but they cannot add or change anything. These users can view BMS anytime and run any of the reports such as nurses, doctors, pharmacy, Medical Center director, Chief of Staff or any other individuals. Administrative group: Members of IS staff who is responsible for bed board setup for the site. This level of access should be restricted to those individuals who would be configuring the BMS system. Administrative and clinical staffs of a Medical Center will use BMS to record, manage and report on the planning, patient movement, patient occupancy, and other activities related to management of beds. All patient admission, discharge and transfer movement are sent directly from VistA to BMS.

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.

Authorized VA clinical staffs and contract employees have access to BMS. Yes, there are contract system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not privileged users of the BMS system itself. All individuals are required to take and maintain their VA training covering NDAs and Rule of Behavior (ROB)s. Contracts are monitored and reviewed by the responsible contracting officer on an on-going basis.

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.

Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and electronic signs he/she will abide by the VA Rules of Behavior. The user also must complete mandatory security and privacy awareness training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* June 9, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* October 17, 2021
5. *The Authorization Termination Date:* October 18, 2024
6. *The Risk Review Completion Date:* September 21, 2023
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.***

Yes

Section 9 – Technology Usage

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

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

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

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

No Cloud Technology

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

ID	Privacy Controls
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: 2024.01.25 17:08:33 -05'00'

Privacy Officer, Nancy Katz-Johnson

Hale, John

Digitally signed by Hale, John
Date: 2024.02.09 08:50:35 -05'00'

Information System Security Officer, John Hale

TONY SINES

Digitally signed by TONY SINES
Date: 2024.02.12 13:08:02 -06'00'

Information System Owner, Tony Sines

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 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 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."

Notice is also provided in the Federal Register with the publication of the SORN: SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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 Handbook 1605.04: Notice of Privacy Practices