Privacy Impact Assessment for the VA IT System called:

Bed Management Solution (BMS)

OI&T Enterprise Program Management Office (EPMO) Veterans Health Administration

Date PIA submitted for review:

9-20-2021

System Contacts:

<table>
<thead>
<tr>
<th>Title</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>John Hale</td>
<td><a href="mailto:John.Hale4@va.gov">John.Hale4@va.gov</a></td>
<td>859-233-4511 x3517</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Christopher Brown</td>
<td><a href="mailto:Christopher.Brown1@va.gov">Christopher.Brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
Abstract

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

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN cover cloud usage or storage?

The mission of the Veterans Affairs (VA) and Office of Information & Technology (OI&T) is to provide Bed Management System (BMS) software to all VA Medical Centers. BMS is a real-time, user-friendly Web-based Veterans Health Information Systems and Technology Architecture (VistA) interface for tracking patient movement, bed status, bed availability, identification and anticipation of peak demands. It provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMC).
An estimated of 350 to 400 Veterans at each VA Medical Center nationwide are registered on BMS. These factors include the nature of a Veteran's discharge from military service (e.g., honorable, other than honorable, dishonorable), length of service, VA adjudicated disabilities (commonly referred to as service-connected disabilities), income level and available VA resources among others.

VistA is an enterprise-wide information system built around an Electronic Health Record (EHR). BMS feeds all bed status information into VistA via a unidirectional procedure in order to provide supports and efficient flow operations in VAMCs. The BMS system’s legal authority for operating the system, specifically the authority to collect the information listed is the President's Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.). The legal authority for use of the SSN is Title 38, United States Code, Section 501 (SORN 24VA10P2 Privacy Act of 1974, 5 U.S.C. 552a(e) and 79VA10P2).

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.

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)
Additional Information Collected:
Patient sex, health condition, and admitting diagnosis.

PII Mapping of Components

BMS consists of five key server components per environment – 2 application servers, 2 SQL servers, 1 web server each for Production and Pre-Production. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by BMS and the functions that collect it are mapped below. The 210/410 sql servers serve as the primary database server, the 211/411 sql servers provide reporting capabilities. The app 210/211, 410/411 servers serve as hosts for the services running primary services and data marshalling for BMS. The web 210/410 servers handle web operations for the BMS application. BMS, BMS_EIS, BMS_DW, BMS_DS, and BMS_HISTORY databases contain PII/PHI.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>VaaussqIbms210.aac.dva.va.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, DOB</td>
<td>BMS collects PII because .. “[to] provide [a] real time, web-based system for VA clinical staffs to record, manage, and report on the planning, The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel</td>
<td></td>
</tr>
<tr>
<td>Vaaussqlbms211.aac.dva.va.gov</td>
<td>YES</td>
<td>NO</td>
<td>Name, SSN, DOB</td>
<td>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 Medical Centers (VAMCs).</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----</td>
<td>----</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>

The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations.
| Vaausappbms210. | YES | YES | Name, SSN, DOB | 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 Medical Centers (VAMCs). | The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations. |
| aac.dva.va.gov | | | | |
| Vaausappbms211. | YES | YES | Name, SSN, DOB | 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 | The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations. |
| aac.dva.va.gov | | | | |
that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs). Information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Access</th>
<th>Name</th>
<th>BMS Collects PII because</th>
<th>The Potential Harm is Mitigated by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaauswebbms210.aac.dva.va.gov</td>
<td>YES NO</td>
<td>Name, SSN, DOB</td>
<td>“[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).”</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Name</th>
<th>Access</th>
<th>Name</th>
<th>BMS Collects PII because</th>
<th>The Potential Harm is Mitigated by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaaussqlbms410.aac.dva.va.gov</td>
<td>YES YES</td>
<td>Name, SSN, DOB</td>
<td>“[to] provide [a] real time, web-based system for VA clinical staffs to record,”</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and</td>
</tr>
</tbody>
</table>
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).

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 Medical Centers (VAMCs).

Vaaussqlbms411.aac.dva.va.gov Yes No Name, SSN, DOB

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 Medical Centers (VAMCs).

The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations.
<table>
<thead>
<tr>
<th>System Name</th>
<th>Access</th>
<th>PII Collected</th>
<th>Purpose</th>
<th>Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaausappbms410. aac.dva.va.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, DOB</td>
<td>BMS collects PII because &quot;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).&quot;</td>
</tr>
<tr>
<td>Vaausappbms411. aac.dva.va.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, DOB</td>
<td>BMS collects PII because &quot;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.&quot;</td>
</tr>
</tbody>
</table>
bed availability. It also provides performance information that can be used to improve patient flow within, and between, VA Medical Centers (VAMCs).

| Vaauswebbms410. aac.dva.va.gov | Yes | No | Name, SSN, DOB | 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 Medical Centers (VAMCs). |

The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. In addition, BMS is an internal-facing system in the VA Intranet with access controlled by role designations.
1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

Data Quality:

a) 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.

b) 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.

c) 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 Handbook 1605.1 outlines policy for processing amendment requests. Other policies, such as VHA Handbook 1907.01 outlines how health records are updated including administratively due to errors.

d) Agency Level - VA ensures and maximizes the quality, objectivity, utility, and integrity of information disseminated to the public. Additional levels of quality standards will be adopted for specific categories of information. VA provides an administrative procedure to allow affected
persons to seek and obtain, where appropriate, corrected information and to appeal contested decisions.

Consent:

a) VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required, VHA obtains signed written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI.

b) The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary and explains the consequences of not providing the information when data collection is voluntary. In addition, for various programs, including Human Subjects Research, appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use and retention of PII and PHI are made as part of the informed consent process.

c) VHA uses and disclosures collected PII as authorized by the Privacy Act, 38 USC Sections 5701 and 7332, and the HIPAA Privacy Rule. VHA Directive 1605.01 outlines policy and procedures for VHA and its staff to use and disclose PII, including with authorization and without authorization. Facilities must comply with applicable federal privacy laws and requirements and uses and disclosures PII in accordance with these laws and VHA Directive 1605.01.

d) VHA uses PII in accordance with all applicable Federal privacy laws and regulations and obtains permission to use PII maintained by VHA as required by those laws and regulations. VHA reviews its SORNs annually and Notice of Privacy Practices periodically to update public notice about VHA’s data collection, use and disclosures of PII.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?
If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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). Additional assistance is available at the following resources:
• The VAMC Health Care System Enrollment Office
• VHA Health Benefits Website
• MyHealtheVet
• VA toll-free 1-877-222-VETS (8387)

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The BMS system does not validate information. The information is trusted as it is being entered into the system from the Veterans through VistA.

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

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 BMS system’s legal authority for operating the system, specifically the authority to collect the information listed is the President’s Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.). Notice is provided by the system’s System of Record Notice (SORN), Electronic Document Management System (EDMS)-VA, VA SORN 79VA10P2: Title 38, United States Code, section 7301(a), and 24VA10P2: Title 38, United States Code, Sections 501(b) and 304 that covers Veterans/Dependents which can be viewed at the following links:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The 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.

**Mitigation:** 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 this facility’s 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 will be used in support of the program’s business purpose.

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*

*This question is related to privacy control AP-2, Purpose Specification.*

Name: Veteran’s identification
Social Security Number (SSN): Veteran’s identification
Date Of Birth (DOB): Veteran’s identification
Mailing Address: Veteran’s address
ZIP: Veteran’s zip code
Ward occupancy: Reviews list of bed assignments, records patient’s movement and notifies that bed is assigned to the Veterans
Bed grouping: Group of bed for the ward to view within a unit
Scheduled admission: information includes scheduled admissions, anticipated discharges, available beds, closed beds, isolation, flight risk patients or SI patients, restrained patients, gender, and patient’s length of stay.
Bed status Tracking bed availability, ready for cleaning, in use, etc.
Integrated sites: Medical center facility and site
2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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.

2.3 How is the information in the system secured?

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.

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access
documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

The minimum-security requirements for BMS’s high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans’ information is used, stored, and protected.

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.

**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
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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.

All electronic records are kept indefinitely per Office Inspector General (OIG) guidance.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

The data retention period has been approved by NARA and is processed according to the following:
- Records Control Schedule VB-1, Part II Revised for VBA:
3.4 What are the procedures for the elimination of SPI?

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

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](http://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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research*

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.

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 3.10 (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**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VistA</strong></td>
<td>Querying of Veterans information for admission, discharge, occupancy data and transfer.</td>
<td>Name Social Security Number Date of Birth Patient sex Health condition Admitting diagnosis</td>
<td>VistA Integration Adapter (VIA)</td>
</tr>
<tr>
<td><strong>National Utilization Management Integration (NUMI)</strong></td>
<td>NUMI Service • Call&lt;Inpatient&gt;(PII/PHI/SPI) • SSN • Level of Care • Review Date</td>
<td>NUMI Exchange</td>
<td></td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

**Privacy Risk:** There is a risk that 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 3.11 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**

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing.

Follow the format below:

Privacy Risk: N/A

Mitigation: 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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Notice is provided by the system’s System of Record Notice (SORN), Veterans Health Information Systems and Technology Architecture 79VA 10P2 and 24VA10P2 that covers Veteran / dependent health information. Links below:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF

Section 6 of VHA Directive 1605.01 also ensures individuals receiving care at a VHA facility are provided adequate notice of VHA’s privacy practices. Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices, is provided by the Health Eligibility Center (HEC), along with information on enrollment, to all Veterans enrolling in VHA for the first time. An individual has the right to request a copy of VHA Notice of Privacy Practice at any time. The notice of privacy practices details the uses and disclosures of the individual’s individually identifiable health information that may be made by VHA, as well as the individual’s rights, and VHA’s legal duties with respect to individually identifiable health information.

VHA also provides a copy of the VHA Notice of Privacy Practices (NOPP) to all non-Veteran patients (e.g., humanitarian, non-VA research subjects, caregivers, and Service members receiving care or treatment at a VHA health care facility) at the episode of care when the non-Veteran patient checks in for an appointment or when the non-Veteran patient is admitted to the hospital. All non-Veteran patients must acknowledge receipt of the VHA Notice of Privacy Practices per VHA Handbook 1605.04, Notice of Privacy Practices.

A copy of IB 10-163 can be found on the VHA Publications website at the following link: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048

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

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 request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is a risk that 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?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.
If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

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
For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

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

**Principle of Individual Participation:** Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

**Privacy Risk:** There is a risk that the individual accidentally provides incorrect information in their correspondence.

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

### Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.
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. Several levels of access are:

**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 ROBs. 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?

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date, 
6. The Risk Review Completion Date
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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


Section 9 – Technology Usage

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

9.1 Does the system use cloud technology?
If so, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

No Cloud Technology

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

N/A

9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

N/A

9.4 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

9.5 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

9.6 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
### Summary of Privacy Controls by Family

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

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

RITA K GREWAL
114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.09.27 09:27:07 -04'00'

Privacy Officer, Rita Grewal

John E Hale
156613

Digitally signed by John E Hale 156613
Date: 2021.09.27 09:50:46 -04'00'

Information Systems Security Officer, John Hale

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.09.27 10:42:12 -05'00'

System Owner, Christopher Brown
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).

Notice is provided by the system’s System of Record Notice (SORN), Veterans Health Information Systems and Technology Architecture 79VA 10P2 and 24VA10P2 that covers Veteran / dependent health information. Links below:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF


Section 6 of VHA Directive 1605.01 also ensures individuals receiving care at a VHA facility are provided adequate notice of VHA’s privacy practices. Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices, is provided by the Health Eligibility Center (HEC), along with information on enrollment, to all Veterans enrolling in VHA for the first time. An individual has the right to request a copy of VHA Notice of Privacy Practice at any time. The notice of privacy practices details the uses and disclosures of the individual’s individually identifiable health information that may be made by VHA, as well as the individual’s rights, and VHA’s legal duties with respect to individually identifiable health information.

VHA also provides a copy of the VHA Notice of Privacy Practices (NOPP) to all non-Veteran patients (e.g., humanitarian, non-VA research subjects, caregivers, and Service members receiving care or treatment at a VHA health care facility) at the episode of care when the non-Veteran patient checks in for an appointment or when the non-Veteran patient is admitted to the hospital. All non-Veteran patients must acknowledge receipt of the VHA Notice of Privacy Practices per VHA Handbook 1605.04, Notice of Privacy Practices.

A copy of IB 10-163 can be found on the VHA Publications website at the following link: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048