



Privacy Impact Assessment for the VA IT System called:

Salesforce - HIT SME Management

VA Electronic Health Record Modernization Integration Office (EHRM IO) - Office of Functional Champion

Veterans Affairs Central Office

Date PIA submitted for review:

07/25/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	(202) 632-8423
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000,4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Health Information Technology (HIT) Subject Matter Expert (SME) Management database is an application that stores contact information for people that have self-identified as Subject Matter Experts (SMEs) interested in participating in VA IT initiatives. This database allows this collected information to be used to support multiple program offices and initiatives within the VA, primarily as it relates to national-level IT projects. The database will assist in assigning these Subject Matter Experts (SMEs) to program office initiatives, using the information collected on these experts to assign them where they can provide the most value.

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 for the system cover cloud usage or storage?*
-
- HIT SME Management is a system owned by the VA Electronic Health Record Modernization Integration Office (EHRM IO) – Office of Functional Champion and controlled by Salesforce.

- The purpose of this IT system is to help assign various subject matter experts (SMEs) to offices, programs, and initiatives where their expertise could be utilized.
- This system is owned by the VA Electronic Health Record Modernization Integration Office (EHRM IO) – Office of Functional Champion and controlled by Salesforce. This system will be used by VA employees at the Office of Health Informatics and EHRM IO.
- The total number of users is approximately 15 internal VA employee users. The application stores contact information (name, work phone, work email, educational history and knowledge areas) for however many people self-identify as Subject Matter Experts (SMEs) interested in participating in VA IT initiatives.
- This database allows the information collected from SMEs (name, work phone, work email, work facility/location, educational history, and areas of expertise) to be used to support multiple program offices and initiatives within the VA, primarily as it relates to national-level IT projects.
- This system has no data shared internally or externally and just holds a database for those 15 team members to help assign SMEs to programs and initiatives.
- This system is only used by one site.
- The Legal Authority to Operate citation Date is 03/18/2021 and the Authorization Termination Date: 12/17/2023.
 - Although HIT SME Management data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF Process, the system has a Data Security Categorization of **Low**, with the impacts of a data compromise being identified in the HIT SME Management system Data Security Categorization (DSC) memo. The Privacy Act is the legal authority to utilize this information.
 - The Privacy Act is the legal authority to utilize this information. [The Privacy Act of 1974](#), set forth at [5 U.S.C. 552a](#), states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.
- The completion of this PIA will not result in any business process or technological changes.
- The completion of this PIA will not result in any business process or technological changes.
- In addition, the SORN does not need to be modified.

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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- | | | |
|---|---|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Financial Account Information | <input type="checkbox"/> Tax Identification Number |
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Medical Record Number |
| <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Account numbers | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Certificate/License numbers | <input type="checkbox"/> Integration Control Number (ICN) |
| <input type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Military History/Service Connection |
| <input type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | <input type="checkbox"/> Next of Kin |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Current Medications | <input checked="" type="checkbox"/> Other Unique Identifying Information (list below) |
| <input type="checkbox"/> Personal Email Address | <input type="checkbox"/> Previous Medical Records | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Race/Ethnicity | |

OTHER Unique Identifying Information: VA Phone Number, VA Email, VA Work Location or VA facility, Educational History, and areas of expertise

PII Mapping of Components

HIT SME Management consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HIT SME Management and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

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 source of information is data directly provided by VA employees, such their self-identified area(s) of subject matter expertise. While the employees will also provide basic contact information and location of work, this information can also be accessed in VA Global Access Location (GAL).

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 technologies 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.*

Contact information such as name, VA phone number, VA email and VA facility/location are all readily available in the VA GAL. Educational history and areas of expertise is self-submitted by the SMEs.

Contact information, including name, VA phone number and VA email are all provided directly by the self-identified subject matter experts (SMEs) who are volunteering to be in the HIT SME database.

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.

Information will be checked for accuracy by the SMEs. Once a SME has agreed to be assigned to a program or initiative, that SME can subsequently indicate whether this program or initiative no longer fits his/her expertise. If they do not request to be subsequently removed, their assignment can be presumed to be accurate. The information will be checked whenever a SME is assigned.

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

When an employee signs a legal contract to work at the VA, they have agreed to have this information collected.

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

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: Employee and Contractor information is stored in this HIT SME Management system. This information may accidentally be accessed by individuals other than the approximately 15 individuals managing the Health Information Technology (HIT) Subject Matter Expert (SME) management database. However, the name, VA phone number, VA email and VA facility/location contained in the HIT SME database are already readily accessible in the VA's Global Access Locator (GAL).

Mitigation: No information is externally or internally shared from this system and no databases are utilized. The HIT SME database is only accessed by approximately 15 users, and those system users have completed VA-required annual standard data safety training. The data obtained for this system (name, work phone and work email, educational history, and areas of expertise) is obtained directly from the VA employees and contractors who voluntarily are included in the HIT SME management system database. Only the minimal amount of information necessary is collected so that HIT SME managers can contact the volunteers should their area of expertise be needed to assist with VA IT initiatives. The data is deemed accurate, complete and current because it is being directly provided by HIT SME volunteers about themselves.

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.

This database allows this collected information to be used to support multiple program offices and initiatives within the VA, primarily as it relates to national-level IT projects. The database will assist in assigning these Subject Matter Experts (SMEs) to program office initiatives using the information collected on these experts to assign them where they can provide the most value.

Name: to use for communication and identification of individual volunteers

Work phone: to use for communication with volunteers

Work email: to use for communication with volunteers

VA facility/location: to use for identifying work location of volunteers

Educational history: to use for identifying knowledge of volunteers

Areas of expertise: to use for identifying subjects that volunteers are experts in

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

Salesforce is used to collate the data. The only data that may be produced is related to SME contact info and their educational history. Salesforce may be utilized to perform data analytics on the HIT SME volunteers. Salesforce Tableau features may be used to visualize or create charts for presentations.

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?

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

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

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

OMB Memorandum M-06-15 applies to the policies for safeguarding sensitive personally identifiable information. Minimal identifying information is being collected for the HIT SME Management database (name, VA phone, VA email, educational history and areas of expertise).

HIT SME Management system (Salesforce) is an encrypted secure system. Data in transit are protected by HTTPS site-to-site encryption. PII data are encrypted at rest with Salesforce Shield encryption, which uses a FIPS 140-2 secure connection.

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.

Access to PII for this system is reserved for VA employees at the VA Electronic Health Record Modernization Integration Office (fewer than 15 people) to assign SMEs to various programs and initiatives. Administrators must approve and provide users with access to the system. Administrators will be responsible for monitoring and safeguarding the system. No data is shared either internally or externally.

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

Information such as name, work phone, work email, work facility/location, educational history and areas of expertise is retained in this system.

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.

Information is retained until an employee retires from the VA or requests to be removed from the HIT SME Database.

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.

Yes, the retention schedule for the Salesforce Development Platform (SFDP) also applies to HIT SME Management.

SFDP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B).

SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records)

The appropriate NARA records retention schedule is as follows:

Skill set records, GRS 2.0 item 120. Disposition instructions: Destroy when business use ceases. DAA-GRS-2017-0007-0018.

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

SMEs can be removed from the database if considered inactive. SMEs can contact the EHRM Office and request removal from the HIT SME database at any time.

There are no physical (paper) records.

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

Yes, this system only uses information that is already stored within VA systems and self-identified educational history and SME specialization. No research or testing will be done using the HIT SME management database. Only employees within the EHRM-IO office will receive training on the system. The system, nor its data, will not be utilized for training for any unauthorized employees.

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: The risk exists that the SMEs' contact information could be accessed by the public or unauthorized individuals. Only the minimal data needed to contact the volunteer SMEs and know their educational history and areas of expertise is retained.

Mitigation: Create a yearly schedule to review the data on file for validity of continued use. If particular education or project history is no longer needed, these data fields can be requested to be expunged. The system utilizes Salesforce Shield 140-2 encryption.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
N/A	N/A	N/A	N/A

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: N/A

Mitigation: N/A

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A	N/A	N/A	N/A	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.

No notice is provided to SMEs. All information is taken from VA Employees or VA Contractors who have voluntarily agreed to be included in the system as a SME and agreed to provide this information. Data collected is limited to name, work phone number, education and areas of expertise.

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

The majority of information is information the person would have provided to the VA prior to working there. Additional educational information or areas of expertise are voluntarily provided by the SME, and each SME's submission only includes the information they choose to include.

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

Yes, individuals have consented to the use of this information through being employed by the VA. SMEs are voluntarily providing their information for the specific use of being included as a subject matter expert (SME) only for the specific areas of self-identified expertise.

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: The risk involves VA employees and VA contractors who voluntarily provide their personal information being unaware that the system retains their name, phone number and work email address. Only VA employees and VA contractors who have voluntarily provided their information are included in the HIT SME Management system, so they have received sufficient notice of the use of their personal identification information.

Mitigation: This system utilizes a FIPS 140-2 connection through Salesforce Shield and also minimizes the PII in the system by only using VA contact information, educational history and areas of expertise. The HIT SME's information is used exclusively for the HIT SME Management system to contact them if their expertise is needed in areas they identified. Their information will not be accessed by or provided to any other VA systems.

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.

An individual would have to be a VA employee or contractor and gain approval to access the system from the system administrator, to have access to this information. Specifically, only VA employees working in the EHRM-IO office responsible for the Functional Champion program will have access the HIT SME Management database system. Those VA employees or VA contractors who have provided their information for inclusion in the HIT SME Management system can contact the Summer Weaver at (816) 615-3424 in the EHRM-IO office at any time regarding the status, accuracy and removal of their personal data from the database.

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.

An individual who volunteered to be included in the HIT SME Management system would inform contact the Summer Weaver at (816) 615-3424 in the EHRM-IO Office of Functional Champion that they are listed as a SME for the wrong subject, and/or inform them that the program/initiative they have been assigned to is not the one they are best suited to assist. A SME volunteer may also request to be removed from the database altogether.

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.

When volunteering to be entered into the HIT SME Management system, volunteers will be told that any changes they wish to make to their information in the system can be corrected by contacting contact Summer Weaver at (816) 615-3424 in the EHRM-IO Office of Functional Champion.

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 ensures data accuracy.

Users can edit their information, by contacting Summer Weaver at (816) 615-3424 in the EHRM-IO Office of Functional Champion.

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.

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: Assigned SME's contact info and educational history is listed in the system. Minimal risk exists because the system is accessed by a small number of VA employees, contains a small number of volunteers' information, and can be readily updated at any time.

Mitigation: This information is protected with Salesforce Shield and any incorrect information can be corrected by an individual notifying the EHRM-IO. VA employees and contractors who have provided their information for inclusion in the HIT SME Management system can contact the EHRM-IO office at any time regarding the status, accuracy and removal of their personal data from the database.

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.

Role-based hierarchy is used for users to access the HIT SME Management application. VA employees can access the tool only after the administrator grants access.

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.

No VA contractors will have access to the HIT SME Management application. VA Contractors' information is retained for assigning to different programs and initiatives through HIT SME Management.

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.

All users of this system have undergone the general VA Privacy 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.***

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 02/24/2021
3. The Authorization Status: ATO
4. The Authorization Date: 03/18/2021
5. The Authorization Termination Date: 12/17/2023
6. The Risk Review Completion Date: 03/12/2021
7. The FIPS 199 classification of the system – Low (L, L, L – C/I/A)
8. Initial Operating Capability (IOC) : 6/20/20217 (legacy System)

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).

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.

Yes, this system utilizes Cloud Computing through Salesforce Government Cloud Plus (SFGCP).

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)

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

Yes, the Cloud Service Provider agreement states that the VA owns the system and Salesforce controls and operates the system. It is under the following agreement: Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.

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.

No Ancillary Data is collected.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

Yes, the Cloud Service Provider agreement clearly states that this is a VA-owned Salesforce-controlled system.

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

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

No RPA is utilized in this system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Tonya Facemire

Information System Security Officer, James Boring

Information System Owner, Michael Domanski

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).

[The Privacy Act of 1974](#), set forth at [5 U.S.C. 552a](#)