Privacy Impact Assessment for the VA IT System called:

Salesforce – National Center for Healthcare Advancement and Partnerships (HAP)

Veterans Health Administration

National Center for Healthcare Advancement and Partnerships (14HAP)

Date PIA submitted for review:

10/03/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
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.

This web-based salesforce application which houses data entered by external-to-VA stakeholders who wish to share innovation proposals with the Center for Healthcare Advancement and Partnerships (HAP). HAP staff employees will access this application and utilize this tool to systematically review the proposal and record actions undertaken for each of the proposals submitted. Actions recorded under each proposal includes but not limited to, completing a due diligence review of the submitter, documenting communications with proposal submitters, receiving input from internal subject matter experts.

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?*

Salesforce – National Center for Healthcare Advancement and Partnerships (HAP) is controlled by Office of Community Engagement (OCE) - National Center for Healthcare Advancement and Partnerships (14HAP). Salesforce Government Cloud Plus (SFGCP) owned in collaboration between Veterans Affairs Central Office (VACO) Information Technology Support Service's (ITSS), Access Management/VA Business Owners and Office of Information Technology (OIT).

HAP is a program within OCE. The mission of OCE is to serve as a trusted resource and a catalyst for the growth of effective partnerships at the national, state, and community level and as a facilitator/access point for public and private entities interested in partnering with VHA to benefit Veterans, their families, caregivers, and survivors. OCE primarily facilitates non-monetary partnerships. The mission of the HAP program is to explore emerging therapies that are safe and ethical to enhance Veteran's physical and mental well-being when other treatments have not been successful. To accomplish HAP's goal, internal and external partnerships are leveraged to provide benefits and services to Veterans.

The HAP app is a web-based portal application. The purpose of the HAP app is to provide the public with a secure tool to share innovative proposals with VA that are intended to benefit Veterans and their beneficiaries directly or indirectly, and facilitate a structured, consistent review of the proposal. Members of the public may enter information into a formatted proposal submission that is accessible online via OCE's public-facing website:
https://www.va.gov/HEALTHPARTNERSHIPS/HAPSubmitaProposal.asp
Once all required information is entered and the proposal is submitted, a new "case" is created in the application, which is then reviewed by OCE staff. OCE staff follow up with proposal submitters to request additional information (if necessary) and to inform them of the results of the proposal review (feasible for implementation/not feasible) and next steps as appropriate.

HAP receives an average of 29 proposals per year and currently stores information on approximately 100 unique proposals. Information shared in a proposal submission includes point of contact (name, telephone number, email address), type, target population (Veteran era, age, beneficiary type), target diagnosis, funding required to implement, current VA partners (if applicable), evidence supporting the innovation and other details relevant to describing the innovation's intended implementation and benefit. Generally, submitters are non-VA affiliated, non-Veteran, members of the public.

After the proposal is shared with HAP, submitters do not have access to their proposal, the database is not accessible outside of the VA network. The application does not link to any other application or database outside of the Salesforce platform. Access to the application is restricted by the application administrator, who is staffed within OCE.

The application is not operated in more than one site.

The following is a full list of related laws, regulations and policies and the legal authorities applicable to the IT System:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information from the SORN: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- VA Directive and Handbook 6502, VA Enterprise Privacy Program

The completion of this PIA will not result in circumstances that requires changes to business processes or technology changes. The system is not in the process of being modified; SORN - 34VA10 / 86 FR33015, “Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA”, (https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf) covers the HAP system. Authority for maintenance of the system: Title 38, United States Code, Section 7301.

The IT System name housing the application is Salesforce Government Cloud Plus (SFGCP) VA Assessing, it is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO). SFGCP VA Assessing is hosted in a Federal Risk Authorization Management Program (FedRAMP) certified cloud called Salesforce Government Cloud Assessing. Salesforce Government Cloud Assessing is maintaining underlying physical infrastructure and was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E). The additional ISA/MOUs established by OI&T and the VA designated contractors/vendors authorized to manage the IT System describe the data ownership and storage requirements. Principles of accountability for the security and privacy of the data are included in the contract documents between the IT System owner and the cloud provider. The magnitude of harm resulting from HAP app data being disclosed is minimal-to-nonexistent, sensitive patient data (PHI/PII) is not stored in the HAP app.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name

☐ Social Security Number

☐ Date of Birth

☐ Mother’s Maiden Name

☐ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Information on the proposal, business name, business phone number, and business email address. VA OCE Staff employees name and email address.

PII Mapping of Components

VHA Salesforce - National Center for Healthcare Advancement and Partnership (Hap) consists of 0 key components (databases). Each component captured by the tool has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HAP 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.

PII Mapped to Components

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					

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.

Individual submitter enters the basis information of name, contact number, email address and proposal on the Salesforce web-application. Pressing the "submit" button on the page generates a case in the application with the information the submitter shared. During the review process, OCE staff employees add notes to the case to capture corresponding information such as communication with the individual, actions taken during the review process, due diligence analysis, subject matter expert review, and any administrative activities.

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.

Information is collected directly from individuals via an online proposal submission template. Individuals who wish to share their proposal with HAP enter the relevant information into the fillable fields on the Salesforce web page (Appendix A).

Prior to promoting the HAP app to the production (live) environment and adding the Salesforce page to the HAP va.gov website, the tool was validated with OMB if the HAP proposal submission page would be considered a "form" under the Paper Reduction Act (PRA). OMB confirmed that the HAP Salesforce page was not a form and was not subject to the PRA.

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.

Proposal submitters are required to input a first name, last name, phone number contact, and email contact for any proposal they choose to share with VA so that OCE staff employees may follow up to request additional information (if necessary) and to inform the submitter of the results of the proposal review (feasible for implementation/not feasible) and next steps as appropriate. Similarly, publicly available and commercial data submitted as part of a proposal, or added to a proposal by the OCE reviewer, is maintained in the record of the proposal. This is to maintain a complete record of all information OCE received from the submitter and to retain all additional details that supported the outcome of the proposal review.

The data and other information stored in the system is not checked for accuracy or compared against any other source of information. Once shared with OCE, details associated with a proposal are not transmitted or shared with any other entity or system.

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 authority for collection and maintenance of information in this system is identified in the System of Record Notice (SORN) 34VA10 / 86 FR33015, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", (https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf) is Title 38, United States Code, Section 7301.

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: Sensitive Personal Information (SPI) including full first and last names and telephone or email contact personal may be released to unauthorized individuals, exposed, or accessed without authorization at the network level.

Mitigation: Profile based permissions control are in place for what data users have access to. Only VA employees' staff at OCE have access to SFGCP VA Assessing, therefore, all users with access to the HAP app will have to complete annual mandatory information security and privacy training to maintain their access. User access to the HAP app on SFGCP is controlled by an administrator within OCE, who grants access limited access following supervisor approval of the request. User access and permissions are reviewed by the administrator on a regular basis to ensure that only users that currently require access have permissions for the HAP app. All data is encrypted in transfer from the Salesforce submission page to the HAP app in SFGCP. Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on secure ports, along with Internet Control Message Protocol (ICMP) traffic and address translation technologies, which further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.

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.

Proposal Point of Contact (POC) data is necessary for communicating with proposal submitters on the status and capture outcome of their proposal.

- First Name: Used to identify the submitter, address them when communicating, and retained for reference.
- Last Name: Used to identify the submitter, address them when communicating, and retained for reference.
- Telephone/Contact Number: Used to identify the submitter, for communication regarding the proposal they submitted, and retained for reference.
- Email address: Used to identify the submitter, for communication regarding the proposal they submitted, and retained for reference.
- Proposal Submission information: Used for proposal review, reporting, and retained for reference.
- VA OCE Staff Employee: Users added case comments, case details, due diligence, and subject matter expert (SME) reviews as part of the review process for consistent evaluation of the proposal, maintaining a record of contact with the proposal submitter, keeping a record of due diligence review on an associated public or private entity (company, non-profit, organization), retaining details related to the proposal from VA SMEs which are integral to the review process and aid in the determination of the proposal review.

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

SFGCP offers basic analysis tools similar in capability to common spreadsheet software. HAP app users can build internal reports and visual dashboards on the SFGCP platform to analyze the number and types of cases submitted, identify how long various stages of the review process take, and can display the workload of assigned and completed cases for each OCE staff member. Reports and visual dashboards are built using data entered in the app. The system does not create or make available new or previously utilized information about an individual. The system does not perform more advanced data analysis functions such as relational analysis, scoring, or pattern analysis. Reports and dashboards are not place in any individual record and do not create new records; they are saved as distinct views of the existing data.

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

HAP 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. SSN is PII data, encrypted at rest with Salesforce Shield encryption.

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.

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA’s stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors.

Access to the HAP app is controlled by an OCE staff member who is assigned as the app Administrator. The Administrator reviews requests for access to the app to verify that the user is a VA employee who has completed the VA Information Security and Privacy trainings. Prior to approving a request for access to the app, the HAP app Administrator also requires approval from the OCE Director or Deputy Director. Access to the app with PII is monitored by the Administrator who edits permissions and removes user access to the app as appropriate.

Additionally, VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook

6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)]

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

HAP salesforce application retains information of VA Employees and Members of Public. First name, last name, telephone/contact number, email address, proposal information and corresponding information relating to the review on proposal submitted.

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.

HAP app data is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule (RCS) 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

As per the SORN applicable for the system, 34VA10: records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition; cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032)

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.

HAP app data is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1" under Records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition; cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032).

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. 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). SFGCP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records).

SFGCP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older than 90 days is unrecoverable. VA can export the data stored on the SFGCP and retain it locally in order to meet VA/NARA retention requirements. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given.

Records in the HAP app can be retrieved using the name of the individual submitter. Upon the individual submitting their information to HAP, a new case with unique case number is created. The case number does include only basic PII information such as name and contact email, records are identified and retrieved by searching for the case numbers.

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

A definitive end of retention period is not defined for RCS 10-1, Chapter 1 § 1115.3 "Primary Program Records". The HAP app does not generate any paper records independent of a use exporting the data to print. Any printed exports of HAP app data by authorized users are considered temporary administrative records and are destroyed when business use ceases.

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

Data stored in the HAP app is not available in testing environments for new applications. SFGCP's testing development sandboxes and testing environment do not have access to HAP record types, therefore, HAP app data is not included in any testing for new applications on Salesforce Government Cloud Plus (SFGCP). The HAP app administrator maintains control for access to HAP app data. Permission to access HAP app data is not granted to developers or administrators for SFGCP application testing. Users accessing the tool would have to undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually.

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 to maintaining data within the HAP app is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, access to the HAP app will be maintained by an Administrator who has completed information security and privacy training. The Administrator will be a VA employee who reports to the Director or Deputy Director of OCE and has completed training on Salesforce app administration. Additionally, the HAP app adheres to the VA RCS 10-1 Schedules. When the retention period is concluded, data stored in the HAP app will be disposed of in accordance with VA and Federal Policy, including the most current version of NIST guidelines for cyber security.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

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

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

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
<u>Privacy Risk:</u> N/A, no information is shared from the system.

<u>Mitigation:</u> 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

List External Program Office or IT System information is	*List the purpose of information being*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system*	*List the legal authority, binding*	*List the method of transmission and the*

shared/received with	***shared / received / transmitted with the specified program office or IT system***		***agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

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

Follow the format below:

<u>Privacy Risk:</u> N/A, no information is shared from the system.

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

Section 6. Notice

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

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

Proposal submitters are informed that the information they submit on the HAP proposal submission page https://www.my.va.gov/ccisubmissionportal will be shared with HAP users. The submission page states, "Use the prompts below to provide details on your innovation. Click the button at the bottom to share your innovation with the Center for Healthcare Advancement and Partnerships." The page also describes how the information will be used (for fair and objective review) and indicates that the submitter will be contacted within 30 days to acknowledge receipt of the submission.

This Privacy Impact Assessment (PIA) also serves as notice of the HAP System. As required by the Government Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

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

Yes, individuals voluntarily submit their information. Information is not requested or solicited; users can decline to share their information by not submitting a proposal to HAP. No penalty or denial of service is incurred from not submitting a proposal to HAP.

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

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

Individuals do have the right to consent to particular uses of the information. Information shared with HAP is only used for proposal review; individuals who do not wish for their information to be reviewed are not required to share their information with HAP.

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 individuals who submit proposals to HAP will not know that the HAP app collects and retains their proposal submission including Personally Identifiable Information (PII).

Mitigation: HAP mitigates this risk by clearly stating on the submission page that information shared in their proposal is sent to HAP and will be reviewed. Individuals are also informed that HAP will contact the proposal submitted to acknowledge the receipt of their proposal and to update the submitter on the status of their proposal's review.

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.

Upon confirmation that HAP has received the proposal from the submitter, the submitter may respond to HAP with a request for access to their information. HAP provides an electronic copy of the submitter's proposal at their request. Individuals are contacted using the OCE shared mailbox CommunityEngagement@va.gov, which is the point of contact for submitters who would like to request a copy of their information. Additionally, users may request a copy of their proposal information through the FOIA/Privacy Act practices, which are linked to on the HAP Proposal Submission Guidelines page: HAP Healthcare Advancement Proposal Submission - National Center for Healthcare Advancement and Partnerships

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.

Upon confirmation that HAP has received the proposal from the submitter, the submitter may request to amend or edit their proposal submission. The process for requesting an editing or correction is the same as described in 7.1 for requesting access to a copy of their submission (CommunityEngagement@va.gov)

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.

Individuals are notified of the procedures for correcting their information upon request by contacting OCE directly. Upon request, OCE will inform individuals that they may correct their information at any time by contacting OCE and providing the information they would like edited or corrected in their proposal submission.

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.

Individuals may request a copy of or corrections to their submission at any time. Access to their submission on the HAP app is not available due to the security protocols used to protect the data.

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: There is a risk that individuals who submit a proposal may mistakenly provide incorrect information which they cannot edit since submitters do not have access to the data stored on the HAP application. Incorrect information may impact OCE's communication with the proposal submitter.

Mitigation: Submitters are informed before they submit a proposal that they will be contacted within 30 days of receipt of their proposal. Upon receipt of a proposal, submitters can communicate directly with OCE to request access, redress, or correction to their proposal. Approvals, denials, and other responses to questions and requests are provided directly by OCE. HAP app data is not shared with other application or entities inside or outside of VA; the information provided by the submitter is not used without their knowledge.

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.

Current SFGCP VA Assessing users can request access to the HAP app through a helpdesk ticket submitted on the SFGCP platform. Only VA employees with completed VA Privacy and Information Security trainings can maintain access to the SFGCP platform. The HAP app Administrator reviews the requests and confirms that access for the user is approved with the OCE Director or Deputy Director. Users from other agencies do not have access to HAP app data. The HAP app Administrator has full access to data in HAP (read/write, edit, delete). Users authorized to access the HAP app have permission to read/write, edit, and delete data that is visible to them depending on the permission granted by HAP Administrator.

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 do not have access to the system or to HAP app data. Contractors do not review proposal submissions and are not granted access to the HAP app record type.

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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance, and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned. Upon approval of access to the HAP app, users receive training on navigating the app and performing fundamental actions (ex: adding a comment, adding due diligence information to a case) from the HAP app Administrator.

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 – Moderate Impact

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, HAP utilizes Salesforce Gov Cloud Plus (SFCGP) Platform as a Service (PaaS) model. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West.

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, VA has full ownership of the PII that will be shared through the HAP app. Contract agreement, “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B.

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 by this tool. VA has full ownership over the data stored in the VA Lighthouse API support system.

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. It is clearly indicated that Salesforce owns and operates the system, VA has full authority over data stored within the 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).

HAP application does not utilize RPA.

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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.10.20 10:57:07 -07'00'

Privacy Officer, Phillip Cauthers

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.10.20 19:42:59 -04'00'

Information System Security Officer, James C. Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.10.27 15:02:16 -04'00'

Information System Owner, Michael S. 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).

HAP proposal submission page: https://www.my.va.gov/ccisubmissionportal

The submission page states:

> All proposals will be fairly and objectively reviewed utilizing extensive evaluation criteria to determine efficacy, feasibility, and originality. Proposal submitters will receive notification that their proposal was received by HAP within 30 days of submission and periodic status updates thereafter. Proposals go through a comprehensive review process and may take several months to review.
>
> Selecting your proposal type will display all the fields applicable to your proposal. Use those prompts to provide your proposal details with HAP. When complete, select the Submit button to share your proposal with the National Center for Healthcare Advancement and Partnerships.
>
> You must enter all REQUIRED information to successfully submit a proposal. Please do not clos your browser window until you are directed by the HAP Submit a Proposal success page.