Privacy Impact Assessment for the VA IT System called:

Access to Care (ATC)

Veterans Health Administration

Business Intelligence Service Line (BISL)

Date PIA submitted for review:

July 21, 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)	Albert Estacio	albert.estacio@va.gov	(909) 583-6309
Information System Owner	Jeremy Gebhard	jeremy.gebhard@va.gov	(360) 566-7302

Abstract

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

The VA Access to Care application provides veterans and other VA customers with up-to-date information on appointment wait times for VA locations within a specified zip code identified by the user. The application uses aggregate data from various VA resources that are already available to the public and displays the information in an easy-to-read format. The system was designed to be a user-friendly application for users to easily find the data in one location and in an easily searchable database.

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 Access.*
- *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?*

The ATC (Access to Care) application's business owner is the Business Intelligence Service Line ("BISL"). BISL is the technical business sponsor. The site was created for the VA Secretary to provide transparency to the public regarding facility wait times, satisfaction rating and quality measures. This application is utilized by the public.

Users access the Access to Care website without authentication and can view the following PII data elements. Estimate of information of about 80,000 individuals stored in the system but numbers will change as providers are added or removed.

• Name
• Occupation
• Service Line
• Gender
• Parent Facility
• Location of Medical Training
• Professional Degree From

The Our Providers data is stored in Azure SQL for the purposes viewing the data on the Access to Care public web site. All data stored in Azure is encrypted with FIPS 140-2 certified algorithms. Access to the Access to Care website is encrypted using TLS/SSL 1.2 communications over HTTPS. The Access to Care system will be operated in the Microsoft AZURE Cloud which has a FedRAMP Joint Authorization Board ("JAB") HIGH P-ATO and a corresponding VA agency authorization. The production components will operate in the MAG Virginia datacenter while the DR components will operate in the MAG Iowa datacenter. The same system and PII controls are implemented across both datacenters.
The completion of this PIA will not result in circumstances that require changes to VA technical or business processes. Access to Care / Our Providers is not a new System of Record (SOR) for storing employee data, but rather is a portal that allows the veteran and the public to search provider data. The application resides in the Azure Government Cloud environment. Azure Government Cloud Service provider has a FedRamp and VA ATO and is rated at FISMA moderate. The VA owns all Access to Care data and there is a BAA with the Cloud Service Provider, Contractors or VA Customers establishing different ownership rights. For additional detail on the agreement between VA and Microsoft with respect to the use of Azure platform services for hosting and storing data refer to the Microsoft Azure FedRAMP ATO package in Risk Vision. Refer to the Microsoft Azure trust center for more information on Compliance, Privacy and Security for Microsoft Cloud Properties. Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer.

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)

Gender; clinical product line to which they are assigned; where providers received their medical training; and the school from which they received their medical degree.

PII Mapping of Components

Access to Care consists of **6** key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Access to Care and the functions that collect it are mapped below.

PII Mapped to Components

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
Our Providers	Yes	Yes	Service providers name, gender, medical school, medical training, clinical serv ice line, and location	This information is beneficial to the Veteran to find VA providers nearest to the veteran	Read only information for user. Admin-role based accounts. Data stored and encrypted at rest
Homepage	NO	N/A	N/A	N/A	N/A
Timeliness	NO	N/A	N/A	N/A	N/A
Satisfaction	NO	N/A	N/A	N/A	N/A
Quality of care	NO	N/A	N/A	N/A	N/A
Overall	NO	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.

Information is provided by VHA to be loaded onto the site in the form of Excel documents. The data is automatically extracted from the Excel document and inserted into the Azure SQL database by way of a cloud service called a data loader. The Site Assistance form is completed by the

external user (veteran) via a web page. The Site Assistance Form website is a way for users to report issues with signing into VA.gov. on other sites. The submitted issue report gets sent into an internal VA CRM DB called Member Services. Member Services is covered by the BAM CRM High ATO not Access to Care. An external user is any internet user, as this form is public, accessible to all, and requires no authentication to use it. The data will then be encrypted and inserted into a processing queue. Another web service will pull the data from the queue, decrypt the data and transmit the data into the VRM ticket system via a webservice call.

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.

The Our Providers and Access to Care components receive information from VHA internal collection and reporting systems containing clinic service information. The information is provided through SQL data replication for publication on the web. The Site Assistance form data is provided by the web user via a web form. Some of the form fields are directed selection (e.g. drop down box), some fields are free-form text. Submission of this data is voluntary.

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.

For Access to Care and Our Providers: Each data load is staged in a User Acceptance Testing (UAT) environment checked for errors and then automatically published to the live site. This system is a derivative data store, the information is obtained from VHA data stores. The information is checked at the point of capture. For the Site Assistance form, many of the fields are directed selection (e.g. drop down box), some of the fields are free-from text. The free form

selection fields will be checked for attempted buffer overrun, code injection, and similar fuzz-testing.

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

Legal authority can be found in Title 38, United States Code, Section 501 and Section 7304: (http://www.gpo.gov/fdsys/granule/USCODE-2011-title38/USCODE-2011-title38-partI-chap5-subchapIsec501/content-detail.html) We have a HIPAA BAA agreement in place with VA in the OST with additional info: https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

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: Loss of Privacy Data - ATC handles employee PII information and there is a risk that the information may be improperly accessed or defaced.

Mitigation: The Access to Care system takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms:
1. The Application's loader API protected by a policy enforcement/policy decision point
2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services.
3. Data -at-rest encryption for any partition where PII will be contained
4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave

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.

VA Provider information is beneficial to the Veteran to find VA providers nearest to the veteran. The Our Providers website is replacing the Our Docs VA hosted site that did not meet the needs of the public as was required to have updated information. The Service Provider information is required so the Veteran can find a provider in a location that is convenient, service line for specialty, providers name and necessary contact info to make an appointment. The Service Providers gender, and medical training aid the veterans that may have a preference. The information in the Site Assistance form will be used to create a service ticket object in the Veterans Relations Management (VRM) customer management system. If, optional, call-back information, both phone and email is provided by the user, the customer service representative will contact the user for assistance. The veterans IP address is automatically logged for security audit purposes only.

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

The only data that is produced by the site is web system logs that log the client IP and URI accessed. This data is ingested into SQL servers for historical analysis and reporting. The Site Assistance form will create an entry in the VRM customer service system.

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?
All data in Azure and on Prem whether stored or in transit is encrypted with FIPS 140-2 certified algorithms. Access to the Access to Care website is encrypted using Transport Layer Security/ Secure Sockets Layer- TLS/SSL 1.2 communications over HTTPS.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? No SSNs are collected.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
The appropriate administrative, technical and physical safeguards are in place to ensure the security and confidentiality of PII/PHI records and to protect against any anticipated threats or hazards to their security or integrity. Data is encrypted in transit and at rest.

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

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

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

<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The minimum-security requirements for the ATC moderate impact system cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA

information systems and the information processed, stored, and transmitted by those systems. Public access to the website is monitored and the user IP address and time is recorded as part of the access auditing. The security-related areas correspond to the NIST SP800-53r4 Control Families:

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

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

Access to Care's Providers data is updated monthly from the provider directory. Any changes to the provider's information would be amended. No individual/patient data is retained by the 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.

Refer to VA Directive 6517 Cybersecurity Management for Cloud Computing Services for additional guidance on VA cybersecurity and FedRAMP policy, as related to all cloud deployments, cloud computing services, cloud computing systems, and cloud computing architectures, operated by, or on behalf of, VA

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.

These records are retained and disposed of in accordance with the General Records Schedule 4-1, approved by National Archives and Records Administration (NARA) (see grs04-1.pdf (archives.gov)

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

Health service provider information is retained and is updated monthly to ensure that provider information is kept current. That information is public information but consolidated on this website for veterans assistance. Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published Records Schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed.

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

ATC does not require you to register or provide personal information in order to visit the web site. The website contains no patient data, and no research, testing, or training is completed with the data."

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: Provider Data could be retained and archived for a longer period of time than necessary.

Mitigation: Access to Care contains Provider data that will be retained for the purposes of historical analysis and reporting such as the clinic wait times. Provider information changes monthly and Individual/Patient data is not retained or processed by the system.. Use of Fed Ramp High controls implemented under the Fed Ramp ATO.

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***
VHA	For Veterans use and convenience	Provider PII-name, location, gender, medical school.	Electronic transmission through VA LAN – all data is encrypted in transit.

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: The Access to Care website is open to the public. There is a risk that information may be accessed by unauthorized individuals or be defaced.

Mitigation: The Access to Care system takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms:
1. The Application's loader API protected by a policy enforcement/policy decision point
2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services.
3. Data -at-rest encryption for any partition where PII will be contained
4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?
Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

Microsoft Corporation	To give Veterans easy access to their information	Contact email address, contact phone number	Cloud Service Provider	Business Partner Extranet (BPE) CIDD307 (connection ID#
Booz Allen Hamilton Government Private Cloud	To provide veterans easy on-line access to their information	Contact email address, contact phone number	Hosting Provider	BPE CID 404

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: There is a risk that information could be accessed by unauthorized individuals.

Mitigation: The Access to Care system takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms:
1. The Application's loader API protected by a policy enforcement/policy decision point
2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services.
3. Data-at-rest encryption for any partition where PII will be contained
4. Data-in-transit encryption using TLS on any network traffic beyond the local enclave.

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.

Access to Care receives its data collection from VA Partner Systems (VHA). SORN # 172VA10 and publication of 86 FR 72688 provides notice to the individual of how the data collected will be utilized within the Veteran Affairs: https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf.
The Site Assistance Component is reached through the VA.GOV website which provides the user notice through the link https://iris.custhelp.va.gov/app/ask. The link provides the following notice at the bottom of the webpage:
The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average ten (10) minutes. This includes the time it will take to read instructions gather the necessary facts and fill out the form. This collection of information is intended to fulfill the need identified by the Department of Veterans Affairs (VA) to categorize your question, complaint, compliment, or suggestion and collect the necessary information to respond to it. Results will be used to automatically route your inquiry to the appropriate person in the VA, which will help ensure that you receive a response in a timely manner. Use of this form is voluntary and failure to participate will have no adverse effect of benefits to which you might otherwise be entitled.

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

Access to Care receives its data collection from VA Partner Systems (VHA). VA Partner Systems (VHA) provide adequate notification by giving public notice of data collection via the Federal Register the Site Assistance component requests voluntary (optional) contact information

if the requesting user wishes to have the support team contact them about their technical support issue. The veterans IP address is registered for security audit purposes only.

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

Access to Care does not provide an opportunity to decline to provide information. Data stored by ATC is received from VA application partners (VHA). ATC does not collect any information directly from Veterans or their dependents.

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 provide information to the Access to Care VA application partners will not know how their information is being shared and used internal to the Department of Veterans Affairs.

Mitigation: SORN # 172VA10 and publication of 86 FR 72688 provides notice to the individual of how the data collected will be utilized within the Veteran Affairs.

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.

In accordance with VA Directive 6300 and Handbooks 6300.3, Procedures for Implementing the FOIA, 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, and VHA Directive 1605.1, Privacy and Release of Information an individual's submitting information requests may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.
Access to Care provider information is publicly available.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are allowed to correct inaccurate or erroneous information by contacting the VA partner system (VHA) in which they are registered. Individuals will follow procedures for correcting individuals' information maintained by VHA. Veteran information collected from the Site Assistance form is not correctable.

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.

By contacting the appropriate VHA office. All requests to review must be received by direct mail, fax, in person, or by email referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures and process as before with the VA Partner system (VHA), and state that the documentation they are now providing supersedes that previously provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: There is a risk that the provider information in Access to Care/Our Providers is inaccurate and decisions are made with incorrect information and that the provider could be unaware of access, redress, and correction procedures.

Mitigation: VA Partner Systems (VHA) follow VA processes which allow an individual, adequate notification of the data being collected and the limitations of use for the data. A formal VA procedure exists where individuals who wish to determine whether this system of records contains information about them should contact the VA facility location at which they are or were employed or made contact. Inquiries should include the person's full name, social security number, dates of employment, date(s) of contact, and return address.

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.

Access to Care \ Our Providers is a publicly accessible web site. The back-end data is only accessible to AZURE contract administrators. The Site Assistance website is a publicly accessible web site. The supporting infrastructure is only accessible to AZURE contract administrators and VA authorized support personnel. The VRM backend components are only accessible to VA authorized support personnel and authorized contractors authorized according to VA policies and procedures

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Yes, there are contract system administration personnel who maintain the cloud infrastructure but are not users of the Access to Care system itself. Contractors sign a NDA for their employment by the vendor and a HIPPA BAA is in place The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. Contractors will have access to this system for development purposes. All contractors are cleared using the VA background investigation process and must obtain a Minimum Background Investigation (MBI). Our Providers and Site Assistance components employ the same security mechanisms.

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.

Clinical provider privacy and security training directives, courses and auditing apply, ensuring individual who have access to PII are trained to handle it appropriately. All individuals must complete all required VA TMS training for Privacy and HIPAA before being onboard to the contract. The training records are retained for 7 years. This documentation and monitoring is performed through the use of the TMS.

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

If Yes, provide: A&A is currently in progress.

YES.

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 11/08/2021
3. The Authorization Status: Authorization to Operate (ATO)
4. The Authorization Date: 9/20/2021
5. The Authorization Termination Date Exp:9/20/2024
6. The Risk Review Completion Date, 11/20/2021
7. The FIPS 199 classification of the system - MODERATE

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

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

Section 9 – Technology Usage

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

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

Microsoft Azure Government – Private Cloud (PaaS)

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

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

Access to Care and VA have ownership rights over data to include PII. Please see the contract between Dell Financial Services and VA. This is the contract that covers the Microsoft Azure Government (Includes Dynamics 365) FedRAMP connection. Access to Care does not have access to the contract at the project level. VA has access to this contract# VA118-17-F-1888.

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 collected or processed

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 ultimate accountability for the security and privacy held by the cloud provider on VA's behalf is described in the BAA contract # VA118-17-F-1888. Department of Veterans Affairs is the owner of all data to include PII for Access to Care. Please see the contract between Dell Financial Services and VA. This is the contract that covers the Microsoft Azure Government (Includes Dynamics 365) FedRAMP connection. Access to Care does not have access to the contract at the project level. VA has access to this contract # VA118-17-F-1888.

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

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

N/A - ATC is not using 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: 2022.08.01 11:35:38 -07'00'

Privacy Officer, Phillip Cauthers

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2022.10.17 11:08:49 -07'00'

Information Systems Security Officer, Albert Estacio

Digitally signed by Jeremy R. Gebhard 331661
Date: 2022.08.05 08:29:36 -07'00'

Information System Owner, Jeremy Gebhard

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).

SORN 172VA10 “VHA Corporate Data Warehouse-VA”,
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf