Privacy Impact Assessment for the VA IT System called:

VetLink (Kiosks)

Office of Integrated Veteran Care (IVC)

Date PIA submitted for review:

July 5, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shonta Wright	Shonta.wright@va.gov	352-372-0906
Information System Security Officer (ISSO)	ChrysAnn Higginbotham	ChrysAnn.Higginbotham@va.gov	573-239-0486
Information System Owner	Angie Wilt	Angela.wilt@va.gov	304-268-6312

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

Abstract

Office of Integrated Veteran Care (IVC) program designs and deploys self-service devices that provide beneficiaries and employees standard, easy-to-use capabilities to improve patient workflow, and to perform clinical and business transactions. Veterans need to receive and provide information in order to manage their health and their relationship with VHA. IVC devices use a software application known as VetLink which enables Veterans to make better use of their wait time at VA locations, to update important information, filing out clinical questionnaires, and providing important information to their care providers.

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:

- *General Description*
  - *A. The IT system name and the name of the program office that owns the IT system.*
    VetLink, VHA Office of Integrated Veteran Care

  - *B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
    The system is aligned under Office of Integrated Access to Care (IVC) office. The Vetlink system is a nationally-deployed patient information exchange software platform that provides Veterans with convenient control of their own health information, while streamlining and standardizing frontline staff and provider activities at VA Medical Centers (VAMCs) and Community-Based Outpatient Clinics (CBOCs) nationwide. Leveraging kiosk capabilities affords Veterans opportunities to elevate the role they play in ensuring the accuracy of information critical to the continued delivery of services. VPS completed national deployment of over 6,300 kiosks in three placement styles (e.g. floor, desktop and wall- intelligent queuing monitors, and 320 servers. The mission of VPS is to provide benefits and services to the 18.2 million Veterans of the United States, includes Alaska, Puerto Rico, Guam, Honolulu, and the Philippines while safeguarding their privacy and enhancing their healthcare experience by providing enhanced capabilities to self-report and participate more fully in their care. In meeting these goals, VPS strives to provide high quality, effective, and efficient clinical and business capabilities, along with Information Technology (IT) services to those persons who are responsible for providing care to the Veterans at the point-of-care. In addition, VPS strives to provide high quality health

care to Veterans throughout all points of their experience in an effective, timely, and compassionate manner. VA depends on a strong business backing, Information Management (IM), and IT systems to meet mission goals. In FY23, the National Program Office decided to continue to maintain the ATO for at a national level; however, the local facilities require to maintain a contract with the vendor (Vecna) to continue operations. Currently, only 40 facilities have a local contract in place and the number of hardware devices have reduced to less than 2,000.

C. Indicate the ownership or control of the IT system or project.

The IT System ownership is partnership with IVC and the 40 facilities that maintain a local contract with the vendor (Vecna). The 40 sites that included in the continuation of the VetLink services are: Bedford, MA; Brockton, MA; Northampton, MA; Jamaica Plains, MA, Manchester, NH; Newington, CT; Providence, RI; Togus, ME, West Haven, CT, West Roxbury, MA, White River Junction, VT; Albany, NY; Batavia, NY; Bronx, NY; Brooklyn, NY; Buffalo, NY; Canandaigua, NY; West Orange/Lyons, NJ; Manhattan, NY; Northport, NY; Syracuse, NY; Atlanta, GA; Augusta, GA (Downtown); Augusta, GA (Uptown); Birmingham, AL; Charleston, SC; Columbia, SC; Dublin, GA; Montgomery, AL; Tuskegee, AL; Tuscaloosa, AL; Tampa, FL; Kansas City, MO; Greater Las Angeles, CA; Long Beach, CA; Prescott, AZ, San Diego, CA; Tucson, AZ; Albuquerque, NM

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The expected number of individuals is estimated to be up to 9 million but is determined by the number of Veterans seeking care at the following locations:: Bedford, MA; Brockton, MA; Northampton, MA; Jamaica Plains, MA, Manchester, NH; Newington, CT; Providence, RI; Togus, ME, West Haven, CT, West Roxbury, MA, White River Junction, VT; Albany, NY; Batavia, NY; Bronx, NY; Brooklyn, NY; Buffalo, NY; Canandaigua, NY; West Orange/Lyons, NJ; Manhattan, NY; Northport, NY; Syracuse, NY; Atlanta, GA; Augusta, GA (Downtown); Augusta, GA (Uptown); Birmingham, AL; Charleston, SC; Columbia, SC; Dublin, GA; Montgomery, AL; Tuskegee, AL; Tuscaloosa, AL; Tampa, FL; Kansas City, MO; Greater Las Angeles, CA; Long Beach, CA; Prescott, AZ, San Diego, CA; Tucson, AZ; Albuquerque, NM. Components collected are name, SSN, mailing address, personal phone number, email address, emergency contact information, health beneficiary information, medical record number, race/ethnicity, next of kin, ePHI, and gender.

E. *A general description of the information in the IT system and the purpose for collecting this information.* Information is collected with prior approval or consent from actual individuals no other sources or commercial data. The purposes of the information from veterans and other members of the public collected, maintained, and processed by the VetLink OS are as varied as the types of information collected. The purposes include:

1. To determine eligibility for health care and continuity of care.
2. Emergency contact information in cases of emergency situations such as medical emergencies.
3. Provide medical care
4. Communication with veterans/patients and their families/emergency contacts

5. Determine legal authority for provides and health care workers to practice medicine and/or subject matter expertise
6. Responding to release of information requests
7. Third party health care plan billing, e.g. private insurance
8. Statistical analysis of patient treatment
9. Contact for employment eligibility/verification

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

The information collected, maintained and/or disseminated by VA Healthcare Record (VistA) comes from a few areas directly from the individual through paper or electronic form and their explicit consent, depending on the type of information. The information may come directly from the Veteran or patient and validated against other prior collected information in programs and resources in the Veterans Benefits Administration (VBA), Health Eligibility Center (HEC), Department of Defense (DoD), Veteran Network Authorization Office (NAO) for non-VA care patients and non-VA medical providers.

G. 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.

AL – Birmingham, AL – Montgomery, AL – Tuscaloosa, AZ – Tucson, AZ – Prescott, CA – Los Angeles, CA - San Diego, CT – Newington, CT - West Haven, FL – Tampa, GA – Augusta, GA – Atlanta, GA – Dublin, MA – Bedford, MA - Jamaica Plain, MO - Kansas City, NH – Manchester, NJ - East Orange, NM – Albuquerque, NY – Albany, NY – Bath, NY – Brooklyn, NY – Bronx, NY – Buffalo, NY – Canandaigua, NY – Northport, NY – Syracuse, RI – Providence, SC – Charleston, SC – Columbia, VT, White River Junction, MA – Brockton, MA - North Hampton, NY – Batavia, ME – Togus, MA - West Roxbury, NY – Manhattan, AL – Tuskegee. The controls 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 include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. Data such as patient wait times, provider case load, and VA employee time and attendance is used to perform daily operational tracking and trend.

3. Legal Authority and SORN, A citation of the legal authority to operate the IT system.

- Veterans Benefit Act, Chapter 73: Veterans Health Administration – Organization and Functions, Title 38 U.S.C §7301.
- Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)
- Veterans' Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
- Veterans' Health Information Systems and Technology Architecture (VistA) Records-VA, 79VA10 (December 23, 2020)
- Enrollment and Eligibility Records-VA 147VA10 (August 17, 2021)

Federal Security Information Act (FISMA), VA Directive 6500, Managing Information Security Risk: VA Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program• Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems 18 U.S.C. 641 Criminal Code: Public Money, Property or Records 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No *SORN is being modified or requires revision.*

D. System Changes

A. Whether the completion of this PIA will result in circumstances that require changes to business processes

No System Changes required; system is in sustainment.

B. Whether the completion of this PIA could potentially result in technology changes

No system changes required; system is in sustainment.

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 Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

ePHI

PII Mapping of Components (Servers/Database)

The VetLink OS consists of two key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VetLink OS and the reasons for the collection of the PII are in the table below.

Internal Database Connections

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
VetLink OS Kiosk	**Yes**	**Yes**	SSN, Name, Mailing Address, Patient Record	**POS**	NIST Security Controls in place AES256

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.
Information is collected with prior approval or consent from actual individuals no other sources or commercial data aggregators.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

N/A

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Information is collected with prior approval or consent from actual individuals no other sources or commercial data aggregators.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information collected, maintained, and/or disseminated by VA Healthcare Record (VistA) comes from a few areas directly from the individual through paper or electronic form and their explicit consent, depending on the type of information. The information may come directly from the Veteran or patient and validated against other prior collected information in programs and resources in the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), Department of Defense (DoD), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers.

1.3b 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.

N/A

1.4 How will the information be checked for accuracy? How often will it be checked?
These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your

organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered an individual's medical record by a doctor or other medical staff is also assumed to be accurate and is not verified.

1.4b 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.

The information collected, maintained, and/or disseminated by VA Healthcare Record (VistA) comes from a few areas directly from the individual through paper or electronic form and their explicit consent, depending on the type of information. The information may come directly from the Veteran or patient, and validated against other prior collected information in programs and resources in the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), Department of Defense (DoD), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers.

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

Veterans Benefit Act, Chapter 73: Veterans Health Administration – Organization and Functions, Title
38 U.S.C §7301.
Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)
Veterans' Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
Veterans' Health Information Systems and Technology Architecture (VistA) Records-VA, 79VA10 (December 23, 2020)
Enrollment and Eligibility Records-VA 147VA10 (August 17, 2021)

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. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The VetLink OS collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.
Mitigation: The VetLink OS, as a minor system, requires that each facility GSS ATO employ a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. VetLink OS relies on the facility's GSS ATO employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives

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.

• Social Security Number: Used as a patient identifier and as a resource for verifying income information with the Social Security Administration• Date of Birth: Used to identify age and confirm patient identity• Personal Mailing Address: Used for communication, billing purposes and to calculate travel pay• Personal Phone Number(s): Used for communication, confirmation of appointments and to conduct telehealth appointments• Personal Email Address: Used for communication• Emergency Contact Information (Name, Phone Number, etc. of a different individual): Used in cases of emergent situations such as medical emergencies• Health Insurance Beneficiary Numbers: Used as a patient identifier and to identify insurance benefits.• Internet Protocol (IP) Address Numbers: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology system to another.• Race/Ethnicity: Used for patient demographic information and for indicators of ethnicity related diseases.• Medical Record Number: Correlates the relevant medical record for the patient.• Next of Kin: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.• Electronic Protected Health Information (ePHI): Used for history of health care treatment, during treatment and plan of treatment when necessary.• Gender: Used to identify gender and confirm patient identity

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

VetLink OS system uses statistics and analysis to create 3 types of general reports that provide the VA with a better understanding of patient care and needs. These are reports are: Version Date: January 2, 2019 Page 5 of 10 Monthly VetLink VAMC and Site Performance Report, VISN Performance Report, and VetLink National Performance Report (Tableau generated reports).

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the

individual? If so, explain fully under which circumstances and by whom that information will be used.

The controls 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 include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. Data such as patient wait times, provider case load, and VA employee time and attendance is used to perform daily operational tracking and trending. ease provide response here

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

At the Enterprise level, only Federal Information Processing Standards (FIPS) compliant encryption methods are used for transmissions. Integrity is provided by use of Wireshark. OIT is responsible for configuring the information system to protect the confidentiality and / or integrity of transmitted information. This can be accomplished by physical means (e.g. implementing protected distribution systems) or by logical means (e.g. implementing encryption techniques). Remote connections must use the VA VPN encrypted tunnel or encrypted Site-to-Site connections.

Security controls implemented to protect data at rest include full disk encryption, virtual disk and volume encryption, and file/folder encryption.

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

All e-mail communications containing SSNs or any sensitive information require encryption using Public Key Infrastructure (PKI) or Rights Management Service (RMS).

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

Authorized users will be provided training as to the appropriate use of the system. Authorized users will only have access to areas of the system that are needed to conduct their duties. User access will be removed when their duties no longer require access.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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.

2.4a How is access to the PII determined?

The controls 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 include mandatory training completion for all employees, volunteers, and contractors.

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

User access criteria, procedures, controls, and responsibilities have been documented as part of the ATO process.

2.4c Does access require manager approval?

Access requires manager approval.

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

Data such as patient wait times, provider case load, and VA employee time and attendance is used to perform daily operational tracking and trending.

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

All authorized users are responsible for assuring safeguards for the PII. Authorized users will be provided training as to the appropriate use of the system.

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

Social Security Number (SSN)
Date of Birth
Health Insurance Beneficiary Numbers /Account Numbers
Internet Protocol Address Numbers
Mailing Address
Race/Ethnicity

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

VetLink OS C will retain patients' health records for 75 years after last episode of medical care, as directed by the Department Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS) 10-1, Part Three, Chapter Six, Code 6000.2(b) (May 2016).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

yes

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

VetLink operates using 2 NARA approved retention schedules•Department of Veterans Affairs, Veterans Health Administration Records Control Schedule 10-1(May 2016) rcs10-1.pdf (va.gov)

•Department of Veterans Affairs, Office of Information & Technology Record Control Schedule005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

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

Information within the VetLink OS is destroyed by the disposition guidance of RCS 10-1. Once the information retention period is reached, Record Management and Office of Information Technology will develop a plan for disposal or deletion. The plan will be routed for approval and implementations through VHA, Veterans Administration Central Office and the National Archives.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No PII is used to test systems prior to deployment. All test is conducted with test samples of the required
application categorization of the subject.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

<u>Principle of Minimization:</u> 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 VetLink OS, is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.
Mitigation: To mitigate the risk posed by information retention, VetLink OS adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4.

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 Medical Centers	Medical Treatment and healthcare services	As described in section 3.1 of this document. i.e. DoB, SSN, Address, benefit, and medical information	VetLink electronically communicated with VA Healthcare System (VistA)

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.
Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

Vecna	System Administration	Date of birth, SSN, address, benefits, medical information	Federal Information Security Management Act (FISMA) VA Directive 6500, Managing Information Security Risk: VA Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security Office of Management and Budget (OMB)	MOU ISA provides approval or interconnection, Vecna utilizes a Cisco ASA 5540 device to create the site-to-site VPN tunnel that connects to the VA Trusted Internet Connection (TIC). This device is FIPS 140-2 compliant. The FIPS 199 Sensitivity Categorization Level is LOW

			Circular A-130, Appendix III, Security of Federal Automated Information	

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 may be shared with an external organization or agency that
does not have a need or legal authority to access VA data.
Mitigation: Safeguards implemented to ensure data is not shared with unapproved or incorrect organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the facilities. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO) and Health Information Management Service (HIMS) to ensure protection of information. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes, notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online:•Veterans' Health Information Systems and Technology Architecture (VistA) Records-VA,79VA10 (Dec 23, 2020)• Enrollment and Eligibility Records-VA 147VA10 (August 17, 2021)

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

Please provide response here

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Yes, notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online:• Veterans' Health Information Systems and Technology Architecture (VistA) Records-VA,79VA10 (December 23, 2020) • Enrollment and Eligibility Records-VA 147VA10 (August 17, 2021)

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 do have an opportunity to decline to provide information at any time. No, there is not a penalty or denial of service for declining to provide information.

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 have the right to consent to uses of information. Individuals are directed to use the 105345 Release of Information form describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories. response here

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that veterans and other members of the public will not know that the VetLink OS exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.
Mitigation: VetLink OS mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. When requesting access to one's own records, patients are asked to complete VA Form 10-5345a:

Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf. Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the myHealthevet program, VA's online personal health record. More information about myHealthevet at https://www.myhealth.va.gov/index.html. In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at http://www.rms.oit.va.gov/sor_records.asp.

.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A. No Privacy Act exemptions apply.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Version Date: January 2, 2019 Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf. Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealtheVet program, VA's online personal health record. More information about MyHealtheVet at https://www.myhealth.va.gov/index.html. In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at http://www.rms.oit.va.gov/sor_records.asp.

.

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 provided the opportunity to submit a request for change in medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer (PO), or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary. Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing.

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.

The SORNs listed in question 6.1 each discuss and notify members of the public of the procedures related to record access, redress, and correction. Links to all VA SORNs can be found at: http://www.rms.oit.va.gov/sor_records.aspIndividuals may request correction of their information by contacting the Facility Privacy Officer, Chief of HIMS, Patient Advocate and/or the Release of Information Office (ROI). Individuals are provided verbal notice of amendment process by the Privacy Officer and/or Health Information Management Systems (HIMS) Chief at time of request. Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: • File an appeal• File a "Statement of Disagreement" • Ask that your initial request for amendment accompany all future disclosures of the disputed health information

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or

group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal Redress is provided. The Privacy Officer provides a written response that includes appeal rights to the individual regarding the outcome if the request is denied. The notification states to contact the Office of General Counsel or VHA Privacy Office regarding the outcome of the amendment request. The individual may also provide a statement of disagreement for the record.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals whose records contain incorrect information may not receive notification of appointments prescription medications, or test results. Furthermore, incorrect information in a health record could result in improper diagnosis and treatments.
Mitigation: VetLink OS mitigates the risk of incorrect information in an individual's records by authenticating information when possible using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

Additionally, VetLink staff is informed of the importance of maintaining compliance with VA Release of Information (ROI) policies and procedures and about the importance of remaining alert to information correction requests.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Individuals receive access to the VetLink OS by gainful employment in the VA or upon being awarded a contract that requires access to GSS systems. Upon employment, the Office of Information & Technology (OIT) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. Veterans Health Administration (VHA) Supervisors are required to review and approve an individual's initial and additional requests for access. Approval process is documented and maintained by the Information Technology (IT) office and the Information Security Officer (ISO).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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, contractors will have access to the VetLink OS. Contracts are reviewed annually by the Contracting Officer Representative (COR). Clearance levels are determined by the COR and position sensitivity level and risk designation. Access is reviewed annually, and verification of Cyber Security training and Privacy is validated by the COR. All contractors and subcontractors are required to sign a VA Form 0752: Department of Veterans Affairs Confidentiality of Sensitive Information Non-Disclosure Agreement prior to beginning any work with the VPS.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All VetLink OS personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training. During New Employee Orientation (NEO) or Via TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* complete
2. *The System Security Plan Status Date: May 16, 2023*
3. *The Authorization Status:* approved
4. *The Authorization Date:* July 16, 2023
5. *The Authorization Termination Date:* July 5. 2025
6. *The Risk Review Completion Date:* March 8, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Currently, the VPS program office is using an Information Assurance GSS authorization as a minor system. The VetLink OS system as a minor system is included as a part of each facility's GSS authorization.
The FIPS 199 Sensitivity Categorization Level is LOW.

- • Confidentiality – LOW
- • Integrity - LOW
- • Availability – LOW

Section 9 – Technology Usage

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

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

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

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

No Cloud technology is used.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

n/a

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

n/a

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

n/a

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

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

n/a

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
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

ID	Privacy Controls
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

SHONTA J. WRIGHT 105740

Digitally signed by SHONTA J. WRIGHT 105740
Date: 2023.08.14 07:50:46 -04'00'

Privacy Officer, Shonta Wright

Digitally signed by ChrysAnn Higginbotham 310049
Date: 2023.08.10 10:06:36 -05'00'

Information System Security Officer, ChrysAnn Higginbotham

Angela R Wilt 103098

Digitally signed by Angela R Wilt 103098
Date: 2023.08.10 10:49:09 -04'00'

Information System Owner, Angie Wilt

APPENDIX A-6.1

VHA Notice of Privacy Practice:

10-163p_(004)_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf

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).

VistA Records-VA 79VA10: 2020-28340.pdf (govinfo.gov)

Enrollment and Eligibility Records-VA 147VA10: 2021-17528.pdf (govinfo.gov)

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices