Privacy Impact Assessment for the VA IT System called:

# VistA Blood Establishment Computer Software (VBECS)

# VA National Pathology and Laboratory Medicine Services (P&LMS)
# Veterans Health Administration (VHA)

Date PIA submitted for review:

05/19/2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Kamilah Jackson | kamilah.jackson@va.gov | 513-288-6988 |
| Information System Security Officer (ISSO) | Jose Diaz | Jose.Diaz4@va.gov | 312-980-4215 |

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Information System Owner | Jeffrey Rabinowitz | Jeffrey.Rabinowitz@va.gov | 732-720-5711 |

## Abstract

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

The VistA Blood Establishment Computer Software (VBECS) version 2 is a tech refresh to the existing version 1 system and movement to a centralized data center (Austin ITC) which migrated to the cloud. This improved Blood Bank software application facilitates ongoing compliance with FDA regulations for medical devices and enhances the Veterans Administration's (VA) ability to produce high quality blood products and services to veterans. The application's primary purpose is to automate the daily processing of blood inventory and patient transfusions in a hospital transfusion service.

## Overview

*The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:*

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

The Sustainment of Blood Bank Maintenance IT system is owned by the Clinical Ancillary Systems program office.

The VistA Blood Establishment Computer Software (VBECS) is an improved Blood Bank software application that facilitates ongoing compliance with FDA regulations for medical devices and enhances the
VA's ability to produce high quality blood products and services to veterans. The application's primary purpose is to automate the daily processing of blood inventory and patient transfusions in a hospital transfusion service

VBECS is hosted on virtualized hardware architecture that is consolidated at two or more data centers. The application reduces the risk of errors through effective use of barcode scanning, retrieval of previous records to be used for comparison, and detection of inconsistencies in data input. It has the capability to provide evaluation of transfusion appropriateness and follow-up on the effectiveness of transfusions rendering improvement on the quality of patient care.

The number of patient records stored in the system increases as new VA patients are added to VBECS because the patient requires blood bank testing or require blood transfusion. Currently VBECS has 291,703,580 records in the production system and 20,419,781 records in the test system. The typical individual affected is a VA patient that requires transfusion of blood or blood products for surgery, chronic illness, or a life-threatening event.

VBECS retains patient's full name, date of birth, gender, and all testing information. This information originates in VistA and is passed to VBECS when a new patient has an order for blood. The information is retained in the VBECS database.

VBECS uses HL7 messaging to share information with other VistA including Computerized Patient Record System (CPRS). The HL7 messaging standard allows the exchange of clinical data between systems. It is designed to support a central patient care system as well as a more distributed environment where data resides in departmental systems. VBECS also uses Remote Procedure Calls (RPC) to exchange data through VistALink with VistA. This data exchange is controlled through Intelligent Character Recognition (ICR) between the Blood Bank medical device software identified by the lowercase "vbec" package namespace in VistA and the "VBECS" package namespace (medical device). VBECS is a national software solution. VBECs servers is hosted in the Azure Cloud

The legal authority to operate VBECS comes from Title 38, United States, Code, Sections 501(a) and 501(b).
Title 21, Code of Federal Regulations, parts 200-299 and Parts 600-680. Title 42, Code of Federal Regulations, section 493.1105.

This PIA will not cause any change in a system of record notice (SORN), business process or technology.

## 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)

Additional SPI collected, used, disseminated, created, or maintained by VBECS includes patient gender and patient laboratory results that pertain to blood transfusion and the Patient's Physician that is ordering transfusions for the patient.

### PII Mapping of Components

Vista Blood Establishment Computer Software VBECS - IO Application Code (VBE) consists of 1 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Vista Blood Establishment Computer Software VBECS - IO Application Code (VBE) and the reasons for the collection of the PII are in the table below

*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 |
|---|---|---|---|---|---|
| **SQL Servers**<br><br>**(132) VAC20SR11VBE201** | **Yes** | **Yes** | **Name, address, date of birth, VA claim number, social security number, military service information, family information, employment information, third party health plan contract information, financial information, medical history** | **Required by FDA regulations for the proper handling of blood products.** | **Limit access to application and database.** All access is done through secure internal VA networks. There is no public facing VBECS platform. All users sign adherence to VA's strict privacy and security controls. Information is shared in accordance with VA Handbook 6500. All |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | employees with access to are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. |

**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 on the Veteran patient comes from the Computerized Patient Record System (CPRS) and the Veterans Health Information Systems and Technology Architecture (VistA)

**1.3 How is the information collected?**

*This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?*

*If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.*
*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

Information is gathered through Health Level Seven (HL7) messages and VistALink lookups

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

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

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

Information is obtained from VistA and CPRS as the original record source. Therefore, the information obtained from VistA and CPRS is considered to be accurate based on the notion that proper accuracy checks were fulfilled in the source systems (VistA & CPRS).

**1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?**

*List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.*
*This question is related to privacy control AP-1, Authority to Collect*

The legal authority to operate VBECS comes from Title 38, United States, Code, Sections 501(a) and 501(b).
Title 21, Code of Federal Regulations, parts 200-299 and Parts 600-680. Title 42, Code of Federal Regulations, section 493.1105. The information and records are used to track the donor medical history, donation interval(s), results of donor testing, report positive or abnormal test results, and blood and/or blood components produced from the donation.

The collection and use of social security numbers is set forth in Executive Order Number 9397. NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL

PERSONS, 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs and 5 U.S.C. 552a - Records maintained on individuals

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
**Privacy Risk:** Sensitive Personal Information including personal contact information, SSN and medical information may be released to unauthorized individuals

**Mitigation:** All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior and the VHA Privacy and HIPAA Focused training annually.

## Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

**2.1 Describe how the information in the system will be used in support of the program's business purpose.**

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

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

- **Name:** Used to identify the patient.
- **Social Security Number:** Used to identify the patient.
- **Date of Birth:** Used to identify age and confirm patient identity.
- **Internet Protocol (IP) addresses:** Used to connect to systems.
- **Current Medications:** Used to determine if effects of testing are related to medication.
- **Patient Gender:** Used to determine clinical significance of Rh antibodies and for transfusion of Rh positive blood in a crisis.
- **Patient Laboratory Results:** Used to proactively review blood product usage and to monitor the effects of transfusion therapy.

**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*

VBECS uses SQL Server for the database and only stores information about the patient for purposes of uniquely identifying data input into the system. VBECS retains records about blood bank test results and blood products that are assigned or transfused to that patient. The data in VBECS is not used for inference or to create new data within the confines of the software.

**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?*

SSN is collected and used as a patient identifier. SSN Data only resides within the VA intranet (not interfaced externally). Only users with EPAS can access the data. The application exposes the data based on defined security role which is managed through a VBECS administrator application's SORN 04VA10P4D (Formerly 04VA115) states the authority to maintain the system is: Title 38, United States Code, sections 501(a) and 501(b). Title 21, Code of Federal Regulations, parts 200–299 and parts 600–680. Title 42, Code of Federal Regulations section 493.1105.

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

SSN is collected and used as a patient identifier. SSN Data only resides within the VA intranet (not interfaced externally). Only users with EPAS can access the data. The application exposes the data based on defined security role which is managed through a VBECS administrator application's SORN 04VA10P4D (Formerly 04VA115) states the authority to maintain the system is: Title 38, United States Code, sections 501(a) and 501(b). Title 21, Code of Federal Regulations, parts 200–299 and parts 600–680. Title 42, Code of Federal Regulations section 493.1105.

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

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

Only users with EPAS can access the data. The application exposes the data based on defined security role which is managed through a VBECS administrator application's SORN 04VA10P4D (Formerly 04VA115) states the authority to maintain the system is: Title 38, United States Code, sections 501(a) and 501(b). Title 21, Code of Federal Regulations, parts 200–299 and parts 600–680. Title 42, Code of Federal Regulations section 493.1105.

**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?*

*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.*

All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior and the VHA Privacy and HIPAA Focused training annually. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's user ID limits the access to only the information required to enable the user to complete their job.

The medical tech users obtain access to VBE by their ADPAC or LIM via an ePAS request. In that request that person says if the new user is an average user or an admin. That request is approved by the CIO for the hospital and the medical director.

## 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*

VBECS retains patient's full name, SSN, date of birth and gender. This information originates in VistA and is passed to VBECS when a new patient has an order for blood. The information is retained in the VBECS database.

**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.*

Retention of records is expected to be 75 years. The information is retained following the policies and schedules of VA's Records Management Service and NARA.

**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.*

VBECS records are retained in accordance with General Record Schedule 2.7 and the Office of Personnel Management Recordkeeping Manual as approved by NARA and CFR - Code of Federal Regulations Title 21 Sec. 820.180 (21CFR820.180) VBECS team confirmed the Retention of Records as seen below

7100.18, 7100.19, 7100.20, 7100.21 and 6000.2 (EHR)

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

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=820.180

**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*

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data:

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

The facility will ensure that sanitization of VA sensitive information from equipment is accomplished before the equipment is released from custody for disposal. This sanitization process must cause the removal of all VA sensitive information from information systems storage devices and render the information from these systems unreadable. The OI&T Chief/CIO will be responsible for identifying and training OI&T staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

**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*

VBECS does not use any live or real data in the development or testing environments.

**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.*

*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**: Handling PII and PHI and retaining for 75 years. Sensitive Personal Identifiable Information (PII) and Personal Health Information (PHI) including personal contact information, SSN and medical information may be released to unauthorized individuals.

**Mitigation:** All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior and the VHA Privacy and HIPAA Focused training annually. Therefore, only users with EPAS authorization can access the data. The application exposes the data based on defined security role which is managed through a VBECS administrator application's SORN 04VA10P4D (Formerly 04VA115) states the authority to maintain the system is: Title 38, United States Code, sections 501(a) and 501(b). Title 21, Code of Federal Regulations, parts 200–299 and parts 600–680. Title 42, Code of Federal Regulations section 493.1105.

## 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*** |
|---|---|---|---|
| CPRS | Clinician places an order for a patient to have a Type and Screen blood test or blood transfusion. | When a new patient has an order for blood, the patient's name, date of birth, hospital location, Social Security Number, and testing information pertinent to blood transfusion is passed to VBECS. | HL7 |
| VistA | Patient medications can affect the serologic results of the Type and Screen blood test. The medication list can assist in explaining test results. | List of medication the patient is taking. | VistALink |
| VistA | Patient information, test results, and patient location, is shared between VistA and VBECS for the purpose | Patient information, test results, and patient location | VistALink |

| *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* |
|---|---|---|---|
| | of record keeping and report generation in both systems. | | |

**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:** Privacy information may be released to unauthorized individuals

**Mitigation:** Access control for VBECS is very limited for PII and PHI. The data already exists in the other systems without VBECS, and the electronic transfers of information are secure. All access is done through secure internal VA networks. There is no public facing VBECS platform. All users sign adherence to VA's strict privacy and security controls. Information is shared in accordance with VA Handbook 6500.

## 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*** |
|---|---|---|---|---|
| N/A -no information is shared outside the agency | N/A | N/A | N/A | N/A |
| | | | | |

## 5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*
*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*
*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:
**Privacy Risk: N/A**.

**Mitigation: N/A**

## Section 6. Notice

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

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

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

VBECS collects all data from other VA IT systems. No opportunity to provide notice exists within VBECS. Veteran patients consent for treatment and medical records when they register for treatment in the VA system.

https://www.oprm.va.gov/docs/Current_SORN_List_1_26_2022.pdf

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

Notice of Privacy Practices IB 10-163

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

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

VHA Directive 1605.01 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Additionally, the NOPP outlines instances when VA may use their information without their consent as captured at the point of care.

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

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

VHA Directive 1605.01 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations.
Additionally, the NOPP outlines instances when VA may use their information without their consent as captured at the point of care.

**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 members of the public may not know that the VBECS system exists within the Department of Veterans Affairs.

**Mitigation:** The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice. Additionally, the publication of this Privacy Impact Assessment (PIA) serves as notice of the VBECS system. All PIAs may be found at:
https://www.oprm.va.gov/privacy/pia.aspx

## Section 7. Access, Redress, and Correction

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

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

*Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.*

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

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

VHA Directive 1605.01 outlines the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

Per System of Records Notice (SORN) 04VA10P4D (formerly 04VA115), SORN 79VA10 and SORN 24VA10A7 Blood donors, patients of VA medical care facilities or duly authorized representatives seeking information regarding access to or who are contesting VA health facility records may write, call or visit the VHA facility where medical service was provided or volunteered.

**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.*

VHA Directive1605.01 outlines the rights of the Veterans to amend to their records The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

Per System of Records Notice (SORN) 04VA10P4D (formerly 04VA115), SORN 24VA10A7 and SORN 79VA10 Blood donors, patients of VA medical care facilities or duly authorized representatives seeking information regarding access to or who are contesting VA health facility records may write, call or visit the VHA facility where medical service was provided or volunteered.

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

**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.*

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.
Per System of Records Notice (SORN) 04VA10P4D (formerly 04VA115), SORN 24VA10A7 and SORN 79VA10 Blood donors, patients of VA medical care facilities or duly authorized representatives seeking information regarding access to or who are contesting VA health facility records may write, call or visit the VHA facility where medical service was provided or volunteered.

**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.*

Formal redress procedure is defined in SORN 04VA10P4D.

Per System of Records Notice (SORN) 04VA10P4D (formerly 04VA115) SORN 24VA1047 and SORN 79VA10 Blood donors, patients of VA medical care facilities or duly authorized representatives seeking information regarding access to or who are contesting VA health facility records may write, call or visit the VHA facility where medical service was provided or volunteered

**7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction**

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

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

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

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

Follow the format below:
**Privacy Risk:** There is a risk that individuals may seek to access or redress records about them held by the VA Office may not have knowledge or awareness of how to request access, redress and correction to their records.

**Mitigation:** By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of the system/application, ensuring the individual has access to the NOPP and staff awareness of where to refer the individuals to exercise their rights.

## 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.*

The VA Wide Area Network (WAN) is protected from unauthorized access. The hardware running the VBECS system and its database will be installed in a secure location to prevent unauthorized modifications and accidental damage.

User roles identify who can access which functions. Not every VBECS user has access to all VBECS options or functions within options. Two or more arrows ( ➢ ) indicate functions limited to a specific role.
It is critical that each site evaluate its staff and determine appropriate security levels based on training and qualifications.

User roles also govern which options are available and which warnings can be overridden. BR_6.02 VBECS displays options that are not available to a user in gray text.

Each of the six user roles is associated with a security level (see Table 1). Privileges accumulate as the security level increases. For example, a Lead Technologist's privileges include those of a Blood Bank Technologist and Enhanced Technologist.

The VBECS users obtain access to VBECS by their ADPAC or LIM via an ePAS request. In that request that person says if the new user is an average user or an admin. That request is approved by the CIO for the hospital and the medical director.

**Table 1: User Roles and Functions**

| Security Levels and User Roles | Accessible Functions | Who Should Fill These Roles? |
|---|---|---|
| Level 1: Blood Bank Technologist (all users) | Activate/edit some shipper information.<br>Activate/edit some blood product information.<br>Standard access (includes patient testing, accepting and canceling orders, modifying units, processing shipments, processing transfusion reaction workups, accessing report functions) | Rotating technologists, new employees, and students trained to perform associated tasks and overrides. |
| ➢➢ Level 2: Enhanced Technologist | Edit unit cost.<br>Modify/issue expired blood products.<br>Release blood products from quarantine. | Experienced technologists trained to process associated overrides and options. |

| | | |
|---|---|---|
| | Edit unit login prior to defining patient associations.<br>Edit verified unit confirmation testing.<br>Edit patient record/verified data and test results (except the ABO/Rh for historic record and the antibody field, which results in an antigen negative requirement).<br>Release directed units to the main blood supply. | |
| ➤➤➤ Level 3: Lead Technologist | Select/issue ABO incompatible blood.<br>Select/issue antigen positive or untyped red blood cells (for the clinically significant antibodies in the table).<br>Print internal reports.<br>Maintain login message. | Experienced technologists trained to process associated overrides and options (e.g., evening- or night-shift supervisors). |
| ➤➤➤➤ Level 4: Traditional Supervisor | Maintain minimum levels.<br>Edit permanent record of the patient's historic ABO/Rh.<br>Edit Transfusion Requirements (TRs) and Special Instructions (SIs).<br>Edit patient record red cell antibody permanent fields (match antigens in the antigen table).<br>Edit a blood unit's record (verified unit data when unit has any previous patient associations).<br>Edit a Patient's Transfusion Record.<br>Remove a Blood Unit's Final Status. | Experienced blood bank supervisors trained to process associated overrides and options |
| ➤➤➤➤➤ Level 5: Enhanced Supervisor | Edit antigen frequency table to reflect local population.<br>Add new local shipper, not already on the table issued with VBECS.<br>Edit and create canned comments for the division.<br>Edit and create consultative reports, templates, MSBOS, reagents, and equipment maintenance logs for the division. | Experienced blood bank supervisors or VBECS administrators trained to process associated overrides and options |
| ➤➤➤➤➤➤ Level 6: Administrator/Supervisor | Define VBECS users' security settings.<br>Define the division as full service or transfusion only.<br>Enable electronic crossmatch at the division.<br>Populate International Council for Commonality in Blood Banking Automation, Inc. (ICCBBA) number for the division.<br>Define valid unit modifications for the division.<br>Assign workload codes for the division.<br>Configure testing.<br>Configure division. | VBECS administrators trained to process all overrides and options not designed to change frequently. This role may be assigned temporarily to a blood bank supervisor at setup to configure the division. |
| VBECS System Administrator (not a VBECS user) | Add users to active directory.<br>Applies maintenance and VBECS patches to the system. | When the division is configured, assign this role only to the System Administrator defined by VA policy 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 personnel who maintain the server hardware and software but are not primary users of the VBECS system itself. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training and the VHA Privacy and HIPAA Focused training (when they have access to protected health information (PHI)) via the VA's Talent Management System (TMS). The office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training and the VHA Privacy and HIPAA Focused training (when they have access to protected health information (PHI)) via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

**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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete the VHA Privacy and HIPAA Focused training annually.

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

*If Yes, provide:*

1. *The Security Plan Status, A signed SSP has been uploaded in eMASS*
2. *The Security Plan Status Date, Oct, 21 2021*
3. *The Authorization Status, 3 Year ATO*
4. *The Authorization Date, Jan,06 2022*
5. *The Authorization Termination Date, Jan 05 2025*
6. *The Risk Review Completion Date, Nov, 15 2021*
7. *The FIPS 199 classification of the system (High)*

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

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

<<ADD ANSWER HERE>>

## 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.*

***VBECS is hosted in VAEC Azure and is covered under the VAEC Enterprise Contract, NNG15SD22B VA118-17-F-2284***

**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.*

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 |
| 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.**

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.08.12 17:55:39 -04'00'

**Privacy Officer, Kamilah Jackson**

Jose Diaz 386249

Digitally signed by Jose Diaz 386249
Date: 2022.08.30 08:39:00 -05'00'

**Information Systems Security Officer, Jose Diaz**

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2022.08.15 11:21:02 -04'00'

**Information Systems Owner, Jeffrey Rabinowitz**

## 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).

https://www.oprm.va.gov/docs/Current_SORN_List_1_26_2022.pdf