Privacy Impact Assessment for the VA IT System called:

BITSCOPIC Platform (BP)

VHA Public Health Surveillance and Research (PHSR)
Veterans Health Administration

Date PIA submitted for review:

2/28/2022

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	kamilah.jackson@va.gov	513-288-6988
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard Alomar-Loubriel@va.gov	787-641-7582
Information System Owner	Angela Gant-Curtis	Angela Gant-Curtis@va.gov	540-760-7222

Abstract

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

The Bitscopic Platform includes several Commercial Off the Shelf (COTS) applications that provide the ability to perform data analytics. Praedico - Public health surveillance, PraediGene - Laboratory workflow and sequencing, PraediTrial - Clinical trial management, PraediCare - Peri-operative analytics and reporting, and PraedAlert - Infection prevention and control. These Bitscopic applications make up the platform and provide high complexity, validated assays for clinical care and public health investigations. The COTS applications are used to manage, expedite, and automate workflows along with related technical work. Complex lab tests are automated for clinical care of VA Veteran patients. The ability to perform RNA (Ribonucleic acid) sequencing and genomic analytics to identify variants of the COVID virus for VA patients is supported. Lastly, the application tracks testing costs and other financial data used by PHSR and supports the reporting of operational statistics to VACO and VHA management. All of the COTS products are licensed from the vendor, Bitscopic Inc.

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 Bitscopic Platform provides high complexity, validated assays for clinical care and public health investigations. The Public Health Surveillance and Research office manages the VA public health processes and reporting using contractor managed systems. The COTS application are used to manage, expedite, and automate the workflow of these assays in PHR along with related technical work. PraediGene is a COTS web application used extensively by the Public Health Reference Laboratory (PHRL) operated by the VHA Public Health Surveillance and Research (PHSR) group located at the Palo Alto Medical Center. PraediGene is a laboratory workflow tool which allows lab staff to electronically enter and track medical lab tests, perform computational biology, and automation of lab test reporting. Work items entered by lab users are immediately available to all personnel for tracking, DNA analysis (when applicable), results and report generation, and workflow control. PraediGene retrieves patient information directly from electronic health record (EHR) systems. The DNA analysis feature automatically predicts and reports resistance mutations based on genetic sequences. PraediGene also generates timely, "EHR friendly" lab test results for reporting to VistA and fully automates clinical, financial, and management reports and records.

Praedico is a COTS web application using data accessed from VistA. The application consists of analytical software used for monitoring infectious disease outbreaks, public health surveillance activities, Veteran influenza reporting, and look-back and epidemiological investigations. The VHA Public Health Surveillance and Research (PHSR) office routinely performs multiple, ongoing clinical trials with the Veteran population serving as patients and subjects.

PraediTrial is a specialized web-based COTS product which successfully automates many clinical processes and optimizes data collection and document management. The planning, protocols, and execution of clinical trials (1) is highly regimented, (2) requires extensive work to select and enroll subjects for the trial, (3) must adhere to numerous regulatory guidelines, (4) involves precise documentation, and (5) is historically a labor-intensive and manual process. PraediTrial is also customized to be used in the VA environment though its ability to interface with VistA data and comply with VA 6550 security regulations. Study sponsors and contract research organizations (CROs) distribute questionnaires to collect information for evaluating whether to invite sites to participate in a study. PraediTrial automates the process of identifying eligible study participants, tracking their questionnaires responses, and maintaining the rigid documentation requirements required for a clinical study.

PraediAlert is a clinical surveillance platform. This software takes in data from multiple systems providing ongoing surveillance and real-time alerts. PraediAlert's features include antimicrobial stewardship, such as drug-bug mismatch and targeted antimicrobial surveillance, as well as infection prevention.

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)
  Internal Entry Number (IEN)

Internal Entry Number (IEN)

PII Mapping of Components

Bitscopic Platform consists of the Public Health Surveillance database. The data collected from internal VA systems and placed in the database has been analyzed to determine if PII is collected. The type of PII collected by **Bitscopic Platform** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

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
VistA	Yes	Public Health Surveillance Database	PII – name, DOB, SSN, IEN, email address, and telephone number PHI – many elements of the EHR	To associate the patient with the clinical sample being tested in the laboratory	Database is encrypted; data encrypted in transit
VHA Telecare System	Yes	Public Health Surveillance Database	PII – name, age, zip code location PHI – Vital signs (body temp, BP, etc.)	To associate the patient with the clinical sample being tested in the laboratory	Database is encrypted; data encrypted in transit
VHA PIMS Systems	Yes	CIS/ARK Database (e.g. PICIS)	PII – name, age, zip code location PHI – Vital signs (body	To associate the patient with the clinical sample being tested in the laboratory	Database is encrypted; data encrypted in transit

			temp, BP, etc.)		

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.

Bitscopic Platform retrieves VistA data from all VistA instances. The Vista data used by Bitscopic Platform is the patient identification (name, SSN, DOB) that is associated with a clinical sample (blood, urine, etc.) submitted to the PHRL for testing. Bitscopic Platform also extracts from VistA the unique accession number assigned to the sample.

Data is not collected from individuals.

No information is 'created' by the Bitscopic Platform.

The Bitscopic Platform only processes identification information from VistA, as well as the test results information created by the PHRL.

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.

Bitscopic Platform retrieves all data and information directly from VistA. The data is retrieved electronically through data extraction and data query processes. In special cases, the PHRL staff may enter the patient identification data manually.

Bitscopic Platform can also import DNA (deoxyribonucleic acid) sequence data from other VA labs around the nation. This collection is performed over the VA internal network using an HL7 protocol. DNA sequence information files contain an anonymized patient identifier associated with the DNA.

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.

PII data collected by the Bitscopic Platform from Vista is always checked for absolute accuracy as it is imperative that the lab test results from PHRL be reported to physicians for the correct patient.

To guarantee total data accuracy, the VistA data for every sample is checked manually against the shipping manifest for that sample when it physically arrives at PHRL.

A second check is performed when the Lab technician scans the bar code (and PII) on the physical sample in to the Bitscopic Platform. Bitscopic Platform then compares the scanned data with the VistA data to ensure absolute accuracy.

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

PHSR accesses data for operational and analytical purposes. Permission to access data is granted through the Veterans Health Administration Director of National Data Systems, Austin Information Technology Center, 1615 Woodward Street, Austin, Texas, 78772, in accordance with the Privacy Act of 1974; System of Records entitled, 24VA10A7 "Patient Medical Records-VA" (Formally known as 24VA10P2)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA"
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
121VA10A7 "National Patient Databases – VA"
https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

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:

The mission of the VHA Public Health Reference Laboratory is to process orders from VA physicians for (1) testing clinical samples to identify infectious diseases amongst Veterans and (2) perform genomic analysis to identify mutations of existing viruses, especially COVID-19.

The Bitscopic Platform does not generate any clinical or patient data. Instead, the required data is copied directly from VistA sites. In rare cases, data may be entered manually by laboratory technicians. In some cases, data is scanned from the bar codes on samples in to the Bitscopic Platform. Only the data necessary to accomplishing the PHRL mission is collected from VistA. No changes are made to the patient or clinical data collected from VistA. Therefore, the policies and procedures for data accuracy and completeness are enforced at the Vista system level prior to its use by the Bitscopic Platform.

While the amount of PII used by the Bitscopic Platform is the absolute minimum needed to accomplish the PHRL mission, there is still an extremely small risk that data could be exposed or corrupted. To prevent any impact to individual patients, the mitigation procedures described below are maintained continuously and for as long as the data reside in the Bitscopic Platform. However, in the case that an unauthorized person obtained access to the patient information, there is the risk of harm to that individual. Specifically, the unauthorized access would be a violation of the patient's privacy and the information could be stolen, causing financial harm to the patient or resulting in a stolen or misused identity.

Mitigation:

In part, the accuracy of the data including quality and integrity relies on the data quality inherited from VistA and the Bitscopic Platform never changes any VistA information and always retrieves the data directly from VistA. Moreover, the Bitscopic Platform adds two additional layers of quality to mitigate any errors. First, all data is manually checked by a lab technician or specialist by comparing the VistA data to the shipping manifests for all samples shipped to PHRL. Then, each sample has their physical label and bar code electronically scanned in to Bitscopic Platform to completely ensure that the VistA data and shipping manifest data fully match the sample label.

Besides these measures to ensure the principal of data quality, the Bitscopic Platform is equipped to ensure data privacy through measures such as (1) strict data access enforcement, (2) isolation of the application from other systems, and (3) being hosted on VA platforms and internal networks that conform to all VA security measures and practices.

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.

The Bitscopic Platform enables the PHSR business mission in the following ways.

First, in the Lab Testing Automation function, the Bitscopic Platform monitors the process of laboratory tests conducted at PHRL. Test specimens (such as blood, nasal swab, urine, tissue, plasma, etc.) are generated at VHA hospital sites. For each specimen, the attending physician orders specific clinical tests to be performed (such as a COVID virus test, HIV, Dengue virus, Zika virus, and so on). Lab specimen's accompanying a provider's ordered test(s) in VistA are shipped to the PHRL Reference Lab at the Palo Alto VAMC.

The Bitscopic Platform pulls information about the physician, the requested tests, and the specimen accession number from VistA. In addition, the PHRL must know the patient for which the test is being conducted. Hence, for each test the Bitscopic Platform extracts the PII needed to track the specimen back to the patient. The required PII is the patient name, date of birth, and SSN.

When the specimen arrives at the Reference Laboratory, a lab technician unpacks the specimen and checks the test/physician information and PII information on the Vista generated shipping manifest. All the information must be accurate and identical. On the specimen itself there is a VistA-generated barcode with the same information. The barcode is read in to the Bitscopic Platform and checked again with the data previously pulled from VistA.

Again, all the information must match precisely. The Bitscopic Platform then produces work orders for the lab for processing the specimen and then tracks each specimen as is processed and records the test date and test results (positive, negative, etc.) in the Bitscopic Platform database for that specimen/patient.

When test procedures are final and the results are approved by a PHRL lab technician, then the Bitscopic Platform will support the reporting of the test results to the ordering physician. This can be done through a LEDI interface connection to the sending VistA site and the patients EHR or it can be done by issuing a printed report for the ordering physician.

In addition to the test assays, the Bitscopic Platform also supports the genomic analysis of COVID-19 samples by identifying the virus's Lineage, Clade and Mutation. The Bitscopic Platform's COVID-Variant Analysis Automation function allows it to accept viral sequence data from Sequence Analyzers at other VHA sites. The Bitscopic Platform then uses analytical techniques to align the sequences for comparison to known COVID variants. The results of this alignment and identification process are then stored on an access-controlled Network Storage Drive. A VistA formatted report is then generated so that the variant analysis results can be reported to the VA physician who requested the test. Throughout this process, the Bitscopic Platform associates the virus's genomic data being processed with the specific patient to whom it applies. Again, this tracking is accomplished with the patient's name, SSN, and DOB.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The analysis portion of the COVID-Variant Analysis Automation within the Bitscopic Platform is responsible for the genomic analysis of patient specimens. These complex algorithms and analysis operate on genome sequences using the manufacturer's proprietary tools and techniques. The result of the analysis is to identify any COVID or other virus variants. Throughout this process only anonymized DNA sequence data is processed. Although no patient identifications are present, the patient DNA and genome data is considered sensitive and is at risk. The genome data is only associated with an anonymous patient UID generated by VistA.

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?

Data stored in the Bitscopic Platform is encrypted.

Bitscopic Platform data collected from VistA is encrypted in transit only when being moved across the VA intranet. The security measures and encryption policies of the VA are used during this transit.

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

There are no additional protections in place.

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

PII/PHI is encrypted in transit and at rest.

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Add answer here:
Access to the Bitscopic Platform and its PII contents is strictly controlled at multiple levels.

1. Access is granted only to members of the following groups:
   - PHRL essential staff and users including lab technicians, the lab manager, and physicians
   - Certain other critical PHSR employees such as IT Specialist, Project Manager, or the PHSR Director
   - Limited staff from the COTS manufacturer have access to the application. Vendor access is limited to the terms of their Business Associate Agreement with the VA.

2. Access is granted only to users who have (a) completed required background checks and (b) have completed all applicable training (HIPPA, Privacy, Security, etc.) offered by the VA TMS system.

3. Access is controlled by PIV card and 2-Factor authentication. The Bitscopic Platform is PIV-enabled in accordance with OIT standards.

4. In addition to PIV authentication, an authorized users list is maintained by the Bitscopic Platform team to control access. The authorized users list of current user accounts is maintained and controlled by PHSR. The Bitscopic Platform denies access to any user who is not on the valid user accounts list.

5. The authorized users list is updated and reviewed by the PHSR IT Specialist on a regular basis.

Access to Bitscopic Platform is granted by the PHSR Director or his designates

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

All PII and data associated with a clinical sample and the lab test results for that sample are retained by the Bitscopic Platform. The retained PII includes the patient's name, SSN, and DOB.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Information is not eliminated from the Bitscopic Platform. Clinical information stored in the Bitscopic Platform is used to generate EHR entries, so it must be retained indefinitely. Moreover, the lab records patient test must be retained indefinitely for use when annual auditing and licensing of the PHRL laboratory takes place.

The Health Records Folder File or CHR (Consolidated Health Record) records series contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The health records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted

to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient health records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Chapter Six Healthcare Records, Item No. 6000.1 (January 2021).

F

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Yes, VA and NARA approved Department of Veterans' Affairs Record Control Schedule (RCS) 10-1.
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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

Information is not eliminated from the Bitscopic Platform. Clinical information stored in the Bitscopic Platform is used to generate EHR entries. Moreover, the lab records must be retained indefinitely for use when annual auditing and licensing of the PHRL laboratory takes place.

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

The Bitscopic Platform is not used for research or for training. Consequently, no PII is being used for these purposes. The Bitscopic Platform is a group of COTS products which is tested before being licensed to the VA. The manufacturer tests their product using contrived or anonymized data to simulate production use by the VA. If the manufacturer needs to test or configure the product using PII, they do so within the VA boundaries on a non-production server under all applicable VA security measures.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk:

The Bitscopic Platform only extracts from the VistA system the minimum PII required for accomplishing PHRL's mission in clinical testing and analytics. These processes have been described earlier in sections 2.1 and 2.2. Unnecessary information or PII is never acquired or stored by the Bitscopic Platform. No PII data is ever shared outside the Bitscopic Platform security boundary or with any other VA system. PII data is only used from the Bitscopic Platform when needed and a user cannot generate any new data to be added to the Bitscopic Platform.

Similar to systems such as VistA or CDW, the Bitscopic Platform needs to retain historical data. Test results become part of a patient health record and must be retained. In addition, lab data must be available for audits, certification procedures, and licensing of the lab. Consequently, the

data is retained indefinitely and in a manner consistent with the Records Management policies governing the data. Similar to other VA systems, the long duration of storing PII in the Bitscopic Platform increases the risk of exposure of that data. Hence, the mitigation measures must be maintained as long as the data is within the system.

Since the data must be maintained for a long period of time, the risk of unauthorized access to sensitive patient information also continues for a longer period. These risks include the potential access and theft of the patient identification which could result in violation of privacy or identity theft and potential financial harm to the patient.

Mitigation:
Data security and privacy risks are mitigated and minimized wherever possible. These measures include strict access control to the system and data and keeping all systems and data on secure OIT infrastructure. Moreover, the vendors use of PII is well controlled and authorized under a national Business Associate Agreement (BAA) between Veterans Affairs VHA and Bitscopic Inc., signed on January 4, 2021.

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***
OIT	To associate the patient with the clinical sample being tested in the laboratory	PII – name, DOB, SSN, IEN, email address, and telephone number PHI – many elements of the EHR	Secure connection using secure socket layer (SSL) with certificates

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

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

Follow the format below:

<u>Privacy Risk:</u>

The sharing of sensitive data is necessary for coordinating Public Health programs across Biosurveillance, laboratory activities, and clinical trials which all combine to contribute to Veteran patient care. However, there is a risk that the data could be shared outside of Public Health with an inappropriate VA organization or institution which would have a potential impact on privacy. The scale of the impact would be dependent on the level of breach associated with risk realized.

<u>Mitigation:</u>

Mitigation is achieved by ensuring that access to the Bitscopic Platform and its PII contents is strictly controlled at multiple levels.

1. Access is granted only to members of the following groups:
   - PHRL essential staff and users including lab technicians, the lab manager, and physicians
   - Certain other critical PHSR employees such as IT Specialist, Project Manager, or the PHSR Director
   - Limited staff from the COTS manufacturer have access to the application. Vendor access is limited to the terms of their Business Associate Agreement with the VA.

2. Access is granted only to users who have (a) completed required background checks and (b) have completed all applicable training (HIPPA, Privacy, Security, etc.) offered by the VA TMS system.

3. Access is controlled by PIV card and 2-Factor authentication. Bitscopic Platform is PIV-enabled in accordance with OIT standards.

4. In addition to PIV authentication, an authorized users list is maintained to control access. The authorized users list of current user accounts is maintained and controlled by PHSR. Access is denied to any user who is not on the valid user accounts list.

1. The authorized users list is updated and reviewed by the PHSR IT Specialist on a regular basis.

Access to the Bitscopic Platform is granted by the PHSR Director or his designates.

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***

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 no external sharing of any information outside the PHSR department. No data leaves the Bitscopic Platform security boundary. No data is shared outside of PHSR and the Bitscopic Platform security boundary

Mitigation:

Not applicable.

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.

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. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis

https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false

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

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

The Veterans' Health Administration (VHA) requests only information necessary to administer benefits to Veterans and other potential beneficiaries. While Veteran, patient or beneficiary may choose not to provide information to VHA, this may preclude the ability of VA to deliver the benefits due those individuals.

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

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

Yes, individuals may request in writing a record restriction limiting the use of their information by filling out a written request. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out.

Individuals can request further limitations on other disclosures. A Veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

VHA permits individuals to give consent or agree to the collection or use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. If individuals are not willing to give information verbally then they are not required to do so. Individuals are made aware of when they must give consent when there is data collected about them through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including that Privacy Act

Statements which are on forms that collect personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations where required. If the individual does not want to give consent then they are not required to in most cases unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VHA obtains a specifically signed written authorization for each intended purpose from individuals prior to releasing, disclosing or sharing PII and PHI.

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 an individual may not receive the NOPP that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA

Mitigation:

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

Individuals must follow established procedures to gain access to their information under the guidelines of the Privacy Act, Freedom of Information Act (FOIA), and Health Insurance Portability and Accountability Act (HIPAA). 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 https://vaww.va.gov/vaforms/. 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 is available at https://www.myhealth.va.gov/index.html.

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 has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VHA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. 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.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

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:

1. File an appeal
2. File a "Statement of Disagreement"
3. Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the facility ROI office or facility Privacy Officer.

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.

A formal redress process via the amendment process is available to all individuals. In addition to the formal procedures discussed in question 7.2 to request changes to one's health 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.

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:
The Bitscopic Platform only uses sensitive information for clinical lab testing purposes and associating a Veteran patient with a clinical sample. Hence, there is no risk to an individual or their healthcare. However, there is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation:
VHA mitigates the risk of incorrect information in an individual's records by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features.

In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access to the Bitscopic Platform and its PII contents is strictly controlled at multiple levels.

1. Access is granted only to members of the following groups:
   - PHRL essential staff and users including lab technicians, the lab manager, and physicians
   - Certain other critical PHSR employees such as IT Specialist, Project Manager, or the PHSR Director
   - Limited staff from the COTS manufacturer have access to the application. Vendor access is limited to the terms of their Business Associate Agreement with the VA.

2. Access is granted only to users who have (a) completed required background checks and (b) have completed all applicable training (HIPPA, Privacy, Security, etc.) offered by the VA TMS system.

3. Access is controlled by PIV card and 2-Factor authentication. The Bitscopic Platform is PIV-enabled in accordance with OIT standards.

4. In addition to PIV authentication, an authorized users list is maintained to control access. The authorized users list of current user accounts is maintained and controlled by PHSR. Access is denied to any user who is not on the valid user accounts list.

5. The authorized users list is updated and reviewed by the PHSR IT Specialist on a regular basis.

Access to the Bitscopic Platform is granted by the PHSR Director or his designates.

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.

VHA Public Health Surveillance and Research (PHSR) licenses the COTS software from Bitscopic Inc. on an annual basis. The contracts to the vendor are reviewed by the PHSR Administrative Officer who also is the COR for the contract. The contract is reviewed and awarded on behalf of the Government by a VA Contracting Officer or Contracting Specialist. Bitscopic's access and use of PHI is authorized under a national Business Associate Agreement (BAA) between Veterans Affairs VHA and Bitscopic Inc., signed on January 4, 2021.

As part of the annual license agreement, the contractor is required to deliver periodic product upgrades, to ensure that data coming into the system is validated and provide support in the event of a software problem. In the process of providing these services, the vendor will view PII and PHI. For this reason, users are restricted as described in section 8.1 above. All vendor users have completed VA background checks and VA privacy training and have VA PIV cards and credentials in accordance with their BAA cited above.

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

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

All users complete the standard, mandatory security training required by the VA. At a minimum, this includes the "Privacy and HIPAA" course and the "VA Privacy and Information Security Awareness and Rules of Behavior" course. Each user attends these courses using the VA Talent Management System 2.0 (TMS) which maintains complete attendance records to ensure that training requirements are fully satisfied annually.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system.*

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.***

The FIPS 199 classication for the system is High. ATO is In Process for the VA Enterprise Cloud (VAEC) Amazon Web Service hosting environment where the Bitscopic Platform will be hosted. ATO expected to be completed by May 30, 2022.

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.

The system will be hosted in VA's Enterprise Cloud (VAEC) Amazon Web Service (AWS), an IaaS.

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

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

Yes, the VAEC contract establishes that VA has ownership rights over the data including PII.

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

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

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

No

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

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

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

Yes. The Information System Owner (ISO) in conjunction with the Information System Security Officer (ISSO), Privacy Officer (PO) and the Information/Data Owner identifies information security and privacy requirements during the requirements analysis based on a specific analysis of availability, integrity, and confidentiality and the technical requirements of the contract. This analysis determines whether contractors or third-party service providers require information access (documents or electronic) in the accomplishment of the VA mission and establishes the appropriate privacy roles responsibilities, privileges, and access rights based on job duties. VA Privacy Service coordinates with Office of Acquisition and Logistics (OAL) and Office of Operations, Security, and Preparedness (OSP) for establishing privacy roles, responsibilities, and access requirements for contractors and service providers and include privacy requirements in contracts and other acquisition related documents. Contractors take privacy and Health Insurance Portability and Accountability Act (HIPAA) training and sign the Rules of Behavior (ROB) before gaining access to VA networks and information in support of contracts.

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).

Not applicable.

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: 2022.04.21 07:49:51 -04'00'

Privacy Officer, Kamilah Jackson

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2022.04.20 17:17:35 -04'00'

Information Systems Security Officer, Richard Alomar-Loubriel

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
Date: 2022.04.20 22:24:04 -05'00'

Information Systems Owner, Angela Gant-Curtis

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://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090