Privacy Impact Assessment for the VA IT System called:

Bitscopic Analytics

Veterans Health Administration

VHA Public Health National Program Office

Date PIA submitted for review:

September 8, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Danny O'Dell	Danny.Odell@va.gov	*650-493-5000 ext 63844*
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 Analytics (BA) security boundary incorporates a toolset of applications used by the VHA Public Health National Program Office (PHNPO) to accomplish the VA's public health mission. BA is composed of three COTS applications.

The Praedico application is used to perform Public Health surveillance and lookback investigations.

The Praedigene application is used to automate and manage activities related to testing patient samples and performing DNA sequencing of pathogens in the Public Health Reference Lab (PHRL).

The PraediTrial application is used to automate certain features and processes for clinical studies conducted by the NPHPO with veteran patient participants. All three 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:

1 General Description
A. The IT system name and the name of the program office that owns the IT system.

Bitscopic Analytics composed of the Praedico, Praedigene, and PraediTrial applications is owned by the VHA Public Health National Program Office (NPHPO)

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*

The Bitscopic Analytics (BA) boundary is comprised of three web-based Commercial-off-the-shelf (COTS) applications used by the VHA Public Health National Program Office (PHNPO). The three systems are Praedico, PraediGene, and PraediTrial. All three applications have been customized for use in the VA, have been interfaced with VistA systems and data, and comply with VA 6550 security regulations.
Praedico collects data from all VistA systems and enables the constant monitoring of veteran health issues and infectious disease outbreaks. Praedico is used to work with immense quantities of patient data combined with complex operations on the data. Praedico provides the analytics needed for accomplishing PHNPO's surveillance and reporting for influenza, COVID-19, and other outbreaks among Veterans and VA staff. Findings and reports are generated by Praedico and enable clinicians and VHA leadership to remain prepared to provide optimal clinical care for patients.

Praedigene - PraediGene is used extensively by the Public Health Reference Laboratory (PHRL) operated by the PHNPO and located at the Palo Alto Medical Center. PHRL is a CLIA-licensed (Clinical Laboratory Improvement Amendments) and CAP-certified (College of American Pathologists) laboratory serving all VA physicians. PraediGene automates the laboratory workflow and allows the lab staff to electronically track clinical tests, perform computational biology, and automate test reporting. Praedigene makes all work items available to lab technicians for tracking, genomic analysis (when applicable), results and report generation, and workflow control. Genomic analysis reports virus resistance mutations based on genetic sequences. PraediGene generates EHR compatible test results for reporting to VistA. Praedigene incorporates a subsystem named PraediVault which serves as biorepository of patient samples processed by the PHRL. PraediVault component of PraediGene performs honest brokering of samples as well as freezer location management of the samples.

Praeditrial - A key mission of the Public Health Office is conducting clinical trials and studies with veteran patients as study subjects. PraediTrial is a specialized tool for automating the identification and recruitment of qualified veteran patients to participate in studies. PraediTrial makes the patient recruitment process faster and more accurate than manual processes. PraediTrial allows a study coordinator or clinical investigator to enter a study plan and criterion for identifying patients who would be appropriate participants in the clinical study. Thereafter, PraediTrial queries VistA to help the study coordinator select candidate patients, then keeps records of the recruitment process, while also maintaining a history of the enrollment actions for each patient.

VA's surveillance responsibilities are mandated by legislative and presidential directives. Legislation, Policies, and Directives include:

- Public Health Security and Bioterrorism Preparedness Response Act of 2002,
- Executive Order 13676,
- Executive Order 13747,
- Fiscal Year 2021 Biodefense Joint Policy Guidance,
- Homeland Security Presidential Directive (HSPD)-5,
- HSPD - 18,
- HSPD - 21,

- National Biodefense Strategy,
- National Biosurveillance Integration Center 6 USC 195(b)(e)(1),
- National Defense Authorization Act for Fiscal Year 2017,
- National Security Presidential Memorandum NSPM–14
- VHA Directive 1131(5) Management of Infectious Diseases and Infection Prevention and Control Programs

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

The Business Owner is the VHA Public Health National Program Office (PHNPO). Control is shared between PHNPO, vendor support from Bitscopic Inc., and VA Office of Information Technology (OIT) infrastructure and services.

2. Information Collection and Sharing

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

Indeterminable. The BA systems will store information from VistA for all veteran patients seen by VA physicians and who have been treated for infectious diseases or have undergone physician-ordered laboratory tests.

E. A general description of the information in the IT system and the purpose for collecting this information.

For surveillance activities the Praedico system collects information for patients who have been treated for infectious diseases, poisonings, etc. as well as the location, age, ethnicity, etc. and identification of those patients. Praedico will also collect EHR information regarding diseases and pathogens, physician diagnosis, patient inoculations, etc. This information is used to analyze and report on pathogen activities across geographic spaces.

The PraediGene application collects data required to process patient specimens and test results on those specimens for test conducted in the Public Health Reference Laboratory (PHRL). When lab tests for patients are ordered by a VA physician, the specimens must be associated with specific patients (PII), their location, and the name of the ordering physician.

The PraediTrial application is used to identify potential participants in clinical trials and clinical studies conducted by the NPHPO. To perform this task, PraediTrial uses

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

The BA tools do not share or send data to any other system outside the BA boundary except for patient data sent back to VistA by the BA tools. BA applications retrieve all data and information directly from VistA. The data is retrieved electronically through data extraction and data query processes. The data collection is performed over the VA internal network using an HL7protocol.

G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

All three applications are hosted at a single site. The system is not a distributed architecture.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

The VHA Public Health National Program Office (formerly known as PHSR) accesses data for treatment, operational and analytical purposes. in accordance with the Privacy Act of 1974; System of Records entitled 24VA10A7 “Patient Medical Record-VA” with authority for maintenance of the system found in Title 38, United States Code, Sections501(b) and 304.

I. *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?*

N/A

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☒ Integrated Control Number (ICN)
☐Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

Age
Immunization Records
Physician Name
Facility
Lab Tests Ordered
Internal Entry Number (IEN)

*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

Bitcopic Analytics components are 34 servers and 1 databases. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Bitscopic Analytics and the reasons for the collection of the PII are in the table below.

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.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Praedigene	Yes	Yes	PII-name, SSN PHI—physician name, facility, tests ordered.	To acquire accurate Patient Medical Records and patient location for surveillance tasks and to ensure lab test results are associated with the correct patient for lab tests. To perform the functions described in Section 1.	Data is encrypted, housed in a VA datacenter, and accessible only to authorized personnel. Data is stored on secure, internal VA databases and storage systems supplied by OIT and compliant with all VA security standards

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?

All data used by the three applications is extracted from VistA systems at each VA hospital site.

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

Bitscopic Analytics (BA) only uses data from VistA. No data from any other source is used or imported to BA.

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

The Praedico application does not create any new information or patient data. Praedico does create public health surveillance reports, studies, and results of look back investigations for infectious diseases. Praedico is a source of information. The PraediGene application produces laboratory test results and genomic sequencing information which becomes part of the patient EHR. Praedigene is a source of information. The PraediTrial application does not create any new patient information or patient-related data. PraediTrial is not a source of information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

All VistA data collection by BA applications is performed over the VA internal network using the HL7 protocol for electronic transmission. All electronic transmissions use secure resources supplied by VA OIT.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

No data is collected by BA on forms or any other non-electronic method. No collection tools are subject to the Paperwork Reduction Act.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Data brought in to the Bitscopic Analytics applications are validated in various ways for both completeness and accuracy.

Data electronically extracted from Vista is initially checked within the applications. These are checks for validity by applying certain rules for recognizing incorrect or invalid data.

Bitscopic Analytics data is then routinely and frequently compared to corresponding data in the VA Corporate Data Warehouse (CDW). CDW queries are performed independently from BA and the results then analyzed and validated by Public Health experts.

Public Health physicians, epidemiologist, and infectious disease specialists also perform random, manual reviews of patient health records via CPRS. The results of random patient chart reviews are used to verify BA data.

PII data collected by PraediGene from Vista is subject to additional tests and 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 patient laboratory sample is checked manually against the shipping manifest for that sample when it physically arrives at PHRL. A second check is performed when the PHRL Lab technician scans the bar code (and PII) on the physical sample in to PraediGene. PraediGene then compares the scanned data with the VistA data to ensure absolute accuracy and consistency.

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

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Bitscopic Analytics does not verify data accuracy using commercial systems or aggregators of any type.

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 VHA Public Health National Program Office (formerly known as PHSR) accesses data for treatment, operational and analytical purposes. in accordance with the Privacy Act of 1974; System of Records entitled, 24VA10A7 “Patient Medical Record-VA” with authority for maintenance of the system found in Title 38, United States Code, Sections501(b) and 304. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.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. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

Bitscopic Analytics applications do 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 Bitscopic Analytics 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 Bitscopic Analytics never changes any VistA information and always retrieves the data directly from VistA. Moreover, Bitscopic Analytics adds additional layers of quality to mitigate any errors.

In rare cases, the Praedigene applications will accept manual data from a lab technician in the PHRL.   In this case, all data is manually checked by a lab technician or specialist by comparing the VistA data to the shipping manifests for all patient samples shipped to PHRL. Then, each sample has their physical label and bar code electronically scanned into Bitscopic Analytics to completely ensure that the VistA data and shipping manifest data completely 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.

Praedico application directly supports the mission and business goals of the VHA Public Health National Program Office (PHNPO) to meet mandated Public Health Surveillance requirements and to provide surveillance, early detection, monitoring, forecasting of infectious disease outbreaks, situational awareness of potentially catastrophic biological events for the purpose of limiting malady, loss of life, and economic impact of diseases.   For surveillance activities the Praedico system collects information for patients who have been treated for infectious diseases, poisonings, etc. as well as the address, zip code, age to include date of birth, ethnicity, social security number, mother's maiden name if applicable, etc. and identification of those patients. Praedico also collects EHR information related to diseases and pathogens, physician diagnosis, lab test results, facility assigned, and patient inoculations. This information is used to analyze and report on infectious disease outbreaks and other biologic events across geographic spaces. All information used by Praedico is internal to the VA.

The PraediGene application is a primary tool enabling the mission of the PHNPO to ensure timely and accurate reporting of laboratory test results and related information back to ordering physicians and patient health records. When lab tests for patients are ordered by a VA physician and conducted by the PHRL, the specimens must be associated with specific patients (PII), their facility, and the name of the ordering physician. All information used by PraediGene is internal to the VA.

Another part of the NPHPO mission is conducting clinical trial and studies that benefit the veteran patients. PraediTrial is the primary tool for supporting the identification and recruitment of qualified veteran patients for study participation. To perform this function PraediTrial accesses VistA patient information including their identification (PII) and certain HER data regarding the medical history of potential study participants. All information used by PraediTrial is internal to the VA.

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

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

The Praedico application does not create any new patient information or data. Praedico is a customizable surveillance, analytics, reporting, visualization and data management platform. There are three functional components to Praedico: integration, discovery and analytics. The integration layer contains a data source connector that can be used to access VistA-extracted data. “Extracted data are integrated to populate the discovery layer which is composed of a data store and database. The database facilitates access to the data stored in the data store in real time. Here data is processed, which includes scrubbing, correlating, standardizing, normalizing, conflating and deduplication using a combination of pre-defined business intelligence rules and machine learning algorithms. The discovery layer can account for semantic variability of data to reduce the incidence of incomplete data pulls due to misspellings and other inconsistencies at the point of entry. Finally, the analytics layer is composed of a point-and-click user interface that allows users to query against the database. Praedico’s analytical capabilities include geospatial mapping of collected data, advanced queries of collected data, and other common surveillance techniques. Analytical results may then be used to generate lookback reports, studies, interactive user dashboards, and other surveillance artifacts.” (Reference: “**Public Health Surveillance in the U.S. Department of Veterans Affairs: Evaluation of the Praedico™ Surveillance System**”, Dr. Cynthia Lucero-Obusan, et al., April, 2021)

The PraediGene application is provided with laboratory test results and genomic sequencing information of viruses which becomes part of the patient EHR. For lab detected pathogens discovered in the patient sample, PraediGene has the ability to compare the pathogen DNA and to DNA of known viruses (via matching algorithms) as well as the clade for the matched virus. The genomic sequencing is performed only when requested by the ordering physician. This information is electronically transferred to VistA via the VA’s standard, secure, encrypted LEDI (Laboratory Electronic Data Interchange) interface for inclusion into the patient’s health record. All other information processed by Praedigene is internal to the application and used for tracking workflow and lab operations, operational costs, lab QA monitoring, and lab schedules.

The PraediTrial application does not create any new patient information or patient-related data. PraediTrial does not perform any complex analysis of data. It is used to help identify potential clinical study participants, organize data for trial participants, and track their activities within a clinical study.

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

The Praedico application does not create any data for any individual.

The PraediTrial application does not create any new data for any individual.

The PraediGene application records results of laboratory tests performed by various testing systems and instruments. Those test results will be sent to the patient's EHR using the VA's standard, secure, encrypted LEDI (Laboratory Electronic Data Interchange) interface. If ordered by a physician, ParediGene can identify pathogen DNA and clade information from the patient sample. This information is retained by PraediTrial and is made available to patient care clinicians and physicians who are authorized to access the patient's EHR.

2.3 How is the information in the system secured?

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

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

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

All data is moved across VA networks and stored on VA storage devices only. Consequently, all devices are secured by OIT and in compliance with VA security standards.

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 and PHI is encrypted in transit and at rest.

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

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

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

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

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

2.4a How is access to the PII determined?

Access to the BA applications and the PII contents is strictly controlled at multiple levels. These include the following procedures:

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 PHNPO 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 (BAA) 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. Access is authorized only by PHNPO leadership.

3. Access is controlled by PIV card and 2-Factor authentication in all cases. All applications are PIV-enabled in accordance with OIT standards.

4. In addition to PIV authentication, an authorized users list is maintained by the BA software to control access. The authorized users list of current user accounts is maintained and controlled by PHNPO. The BA applications deny access to any user who is not on the valid user accounts list.

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

Access to BA applications is granted by the PHNPO Director or his designate.

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

Yes. Procedures are documented and all BA authorized users are known and documented.

2.4c Does access require manager approval?

Yes, by the PHNPO Director or his designate.

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

Yes, system journals track all users who enter the BA applications. No user can enter the application or access any data unless they are on the Authorized Users List.

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

Every individual staff member and employee of the NPHPO is responsible for assuring the protection of PII. Every individual with operational access to the BA applications must complete the "**Privacy and HIPPA Training**" course and the "**VA Privacy and Information Security Awareness and Rules of Behavior**" course offered through the VA Talent Management System (TMS).

Every employee is required to pass this training every year. As such, every employee with access to BA PII information is trained and responsible for assuring safeguards for the PII.

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 indefinitely by PraediGene since this data is part of the patient health records. Praedico and PraediTrial retain PII to include the patient name, SSN, patient DOB, and all the data items indicated previously in section 1.1 and is retained indefinitely.

3.2 How long is information retained?

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

When managing, and maintaining VA data and records, all healthcare facilities will follow the guidelines established in the VA and NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)10-1 found at https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2 Version Date: February 27, 2020 Page 17 of 23 Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008),found at https://www.va.gov/vapubs/search_action.cfm?dType=1 When required, data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Security Handbook 6500.1.

Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, Field Security Service (FSS) Bulletin #344 dated July 24, 2017 for Media Sanitization Program, as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization. (OIT-OIS SOP 0001) OIT/OIS SOP MP-6 Electronic Media Sanitization V4.0].

For information technology and databases, RCS 10-1 is followed. Specifically, Section 2000.1(Information Technology Development Project Records), subsection c ('Special Purpose computer programs and applications) is the governing directive. This regulation requires that BA database records will be destroyed 5 years after the project is terminated, but a longer retention may be required for business use. To date, no BA data has been destroyed since the applications are still active and in daily use by PHNPO.

Additionally, all PII and data associated with a clinical sample and the lab test results for that sample are retained indefinitely by PraediGene since this data is part of the patient health records maintained under RCS 10-1 Sections 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

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

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

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

Yes, VA and NARA approved Department of Veterans' Affairs Record Control Schedule (RCS) 10-1.

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

For Praedico the only records containing sensitive information are stored in the Oracle database used by the application. The disposition authority for these records is DAA-GRS2013-00060005 and DAA-GRS2013-0006000. For operational continuity and data quality purposes, the Oracle data is backed up daily. The backups are securely performed within the VA by OIT using their Commvault backup technology. Backup data has a 7 day retention period and any backup records more than seven days old is immediately destroyed after it has been used.

For Praedigene the only records containing sensitive information are stored in a SQL Lite database used by the application. The disposition authority for these records is N1–15–91–6, Item 1d and N1–15–02–3, Item 3. For operational continuity and data quality purposes, the SQL data is backed up daily. Backup data has a 1day retention period and any backup records more than 1 day old is immediately destroyed after it has been used.

PraediTrial has no saved records containing sensitive information.

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

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

To date, no Praedico data has been destroyed since the project is still active and in daily use by PHSR. In accordance with regulation RCS 10-1, BA database records will be destroyed 5 years after the business use of the project is terminated. At that time, only electronic records will need to be eliminated and they will be disposed of by the VA Office of Information Technology (OIT) in accordance with their procedures.

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

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

The BA applications are not used for research or for training. Consequently, no PII is being used for these purposes.

The applications are COTS products which are tested before being licensed to the VA. The manufacturer tests their products using contrived or anonymized data to simulate production use by the VA. If the manufacturer needs to test or configure the product using actual 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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.

Privacy Risk:

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

Similar to systems such as VistA or CDW, the Bitscopic Analytics boundary applications need to retain historical data. Many of the analytics performed on the data rely on historical records needed to conduct 'look back' investigations and studies of historical public health events. Moreover, the Praedico analytics are frequently used to compare current data and current trends with past years and prior events. For PraediGene, historical data must be maintained to support laboratory audits for annual CLIA certification. Consequently, data is retained indefinitely and in a manner consistent with the Records Management policies governing the data (see section 3.2).

Mitigation:

Data security and privacy risks are mitigated and minimized wherever possible. These measures include strict access control to the system and data (see section 2.3) and keeping all systems and data on secure OIT infrastructure. Also, 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.

To mitigate the risks associated with the length of time the data is retained, the existing security measures described previously are continuously maintained. In addition, time induced risk is mitigated by constantly ensuring that only the essential, minimum data needed by BA is retained. Lastly, time risk can be managed by purging unnecessary data if such data is identified and if the budget resources are available for that effort.

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***
Veterans Health Administration - VistA	To report test results to the	Patients name, DOB, SSN, Patient, Test identifier, IEN, accession number, test date,	Encrypted, secure VA internal network and secure

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***
	physician who ordered the lab test	and test results (positive, negative, etc.)	LEDI interface to VistA

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a “least privilege/need to know” policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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***
There are no interfaces to systems outside the VA; No data leaves the VA	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:

None. No data is shared to any system outside the Bitscopic Analytics security boundary. Data is sent by Praedigene using secure electronic communications and a secure LEDI interface to the VA's VistA system within the VA security boundary.

Mitigation:

None. No data is shared to any system outside the Bitscopic Analytics security boundary. For data sent to VistA, data travels in encrypted form on the VA's secure internal network and through a secure LEDI interface to VistA.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?
These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

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

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. Non Veterans receiving care are provided the notice at the time of their encounter.

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORN 24VA10A7 "Patient Medical Record – VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

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

Notice was provided and can be found here:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

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 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>*Principle of Use Limitation:*</u> *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:

<u>Privacy Risk:</u>

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.

<u>Mitigation:</u>

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?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***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.***

Individuals can gain access to their information through the VA's FOIA and Privacy Act practices and procedures.

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

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.

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

N/A. This system is a Privacy Act System.

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:

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

Information can also be obtained by contacting the Release of Information office at the facility where the Veteran is treated.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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, a veteran or other VAMC patient who is enrolled in myHealth*e*vet can use the system to make direct edits to their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

<u>Principle of Individual Participation:</u> 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.

<u>Privacy Risk</u>:

Praedico only uses information for analysis and infectious disease surveillance activities. 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.

<u>Mitigation:</u>

VHA mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

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?

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

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

Access to the BA applications and the PII contents is strictly controlled at multiple levels. Access to BA applications is granted by the PHNPO Director or his designate. 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 PHNPO 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 (BAA) with the VA.

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. Access is authorized only by PHNPO leadership.

Approved users must have a current PIV card and 2-Factor authentication is always used accordance with OIT standards. In addition to PIV authentication, an authorized users list is maintained by the BA software to control access. The authorized users list of current user accounts is maintained and controlled by PHNPO. The BA applications deny access to any user who is not on the valid user accounts list. The authorized users list is updated and reviewed by the PHNPO IT Specialist on a regular basis.

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

There are no users other than Veterans Affairs. No other agency has access to the Bitscopic Analytics applications.

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

All three BA applications are restricted to Read-Only access to the users. No user can alter the data acquired from VistA.

All three applications provide general use of all application functions for every users. The single exception is the PraediGene application which provides access to financial data for PHNPO management users.

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 Praedico 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 Praedico 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 on an annual basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* March 8, 2023
3. *The Authorization Status:* ATO
4. *The Authorization Date:* May 18, 2023
5. *The Authorization Termination Date:* November 14, 2023
6. *The Risk Review Completion Date:* May 1, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

No.

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

N/A

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

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

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

N/A

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

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

N/A

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

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

No RPA is used

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

ID	Privacy Controls
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.09.28 12:51:24 -07'00'

Privacy Officer, Phillip Cauthers

DANNY M O'DELL 203007

Digitally signed by DANNY M O'DELL 203007
Date: 2023.09.26 14:13:31 -07'00'

Information System Security Officer, Danny O'Dell

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
Date: 2023.09.26 16:06:11 -05'00'

Information System 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).

The VHA Notice of Privacy Practice (NOPP)

SORN 24VA10A7 “Patient Medical Records-VA” https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices