Privacy Impact Assessment for the VA IT System called:

Path and Lab Med (PALM)

VA National Pathology and Laboratory Medicine Program

Veterans Health Administration

Date PIA submitted for review:

10/25/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	William Ponce	William.Ponce@va.gov	720-788-4518
Information System Owner	Robin Nuspl	Robin.Nuspl@va.gov	(858) 472-7317

Abstract

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

Path and Lab Med (PALM) system (middleware) is a necessity for interfacing clinical laboratory medical devices with VistA/CPRS and Cerner as we move forward for the ordering and subsequent reporting of patient lab data. In August 2016 National VistA Patches were released which allow for Auto-Verification processes to be implemented within the clinical pathology laboratory. Universal Interface Software serves as the primary communication hub for auto-verification decision support, including monitoring and selectively altering/routing messages based on user-specified criteria. A standardized, high availability environment to host the Data Innovations Instrument Manager Software that is used as the PALM Generic Interface manager (GIM) to assure connectivity from laboratory instruments to VistA is the best practice to assure the best patient care for our veterans while decreasing cost through site instance consolidation and planning for the future by leveraging the VAEC (VA Enterprise Cloud) AWS (Amazon Web Services) environment using the Path and Lab Med (PALM) system.

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.

Path and Lab Med (PALM), Pathology and Laboratory Medicine

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

Path and Lab Med (PALM) is a universal generic interface manager hosted in the AWS VA Enterprise Cloud, middleware, interfacing laboratory medical devices to the laboratory information system and electronic health record with lab-wide and multi-lab integration. It allows for lean process optimization, interfaced and integrated quality control and quality assurance tools, real-time data analytics for business and clinical decision support, highly reliable system to assure critical laboratory functions are available for laboratory operations.

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

This instance is currently for VISN 22 Pathology and Laboratory Medicine Service under the VISN 22 Pathology and Laboratory Medicine Consolidated Service Line. This Service line consists of the following laboratories:

- RAYMOND G. MURPHY VAMC, Albuquerque, New Mexico
- NORTHERN ARIZONA HEALTH CARE SYSTEM, Prescott, Arizona
- PHOENIX VAMC, Phoenix, Arizona
- SOUTHERN ARIZONA HEALTH CARE SYSTEM, Tucson, Arizona
- LOMA LINDA HCS, Loma Linda, California
- VA LONG BEACH HEALTHCARE SYSTEM, Long Beach, California

- VA GREATER LOS ANGELES HEALTHCARE SYSTEM, Los Angeles, California
- VA SAN DIEGO HEALTHCARE SYSTEM, San Diego, California

2. Information Collection and Sharing

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

The expected number of individuals that could have stored information in this system would be equal to the number of unique patients seen within VISN 22 that have laboratory testing performed. Approximately 300 VISN 22 Laboratory personnel including specimen processing, Medical Laboratory Scientists, Medical Laboratory Technicians, Pathologists and Laboratory Administrative staff utilize the system for clinical and business analytics purposes.

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

SSN, Date of Birth, Race, Sex, Full Name, ordering healthcare provider and location are sent with clinical test orders from VistA/CPRS/Cerner as placed by the veteran's ordering provider. SSN, Date of birth, full name is used to positively identify the specimen with patient. The date of birth, race and sex are used to determine some reference ranges or decision support for laboratory results. Provider and ordering location are used to communicate results as required. Results from the medical laboratory device are received, decision support algorithms may be executed using some of the above information to communicate results, apply reference ranges, add comments, add required reflex testing. Quality control data is sent from medical laboratory devices to Quality Control Management programs. Proficiency Testing Results are sent from medical laboratory devices to accreditation agencies.

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

Quality control data is sent from medical laboratory devices to Quality Control Management programs. Proficiency Testing Results are sent from medical laboratory devices to accreditation agencies. Patient Test results are sent from the laboratory medical devices through Path and Lab Med (PALM)

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.

This system is used in VISN 22 Pathology and Laboratory Medicine Consolidated Service Line, system configuration and functioning is such that the same PII/PHI elements are sent/received across all sites with adherence to the same controls.

3. Legal Authority and SORN

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

System of Record Notice 24VA10A7- Patient Medical Record-VA found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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?*

No update required, yes covers cloud usage/storage

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)

Ordering Provider name
Laboratory Testing Orders/Results
Blood Type
Data File Number (DFN)
Blood Type

PII Mapping of Components (Servers/Database)

Path and Lab Med (PALM) consists of one key component (servers/databases). The type of PII collected by Path and Lab Med (PALM) 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
Data Innovations Instrument Manager primary Interface Server in VAEC AWS using Intersystems Cache	**Yes**	**Yes**	Name, Social Security Number, Race, Gender, Date of Birth, Data File Number (DFN), Laboratory Orders and Results,	Laboratory patient care – to apply appropriate flags, reference ranges, and calculations to lab results. To positively identify patient to laboratory specimen	Data Innovations Instrument Manager primary Interface Server in VAEC AWS using Intersystems Cache

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?

The information is collected or created directly from VistA/Patient Electronic Health Record

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.

The information is collected from the individual but is first entered in VistA/Electronic Health Record during patient enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares.

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

The system receives lab results from the medical devices and in some instances, may modify these results (such as a calculation, added comments, or result translation) which are then sent back to VistA/Electronic Health Record

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?

The information is collected or created directly from VistA/Patient Electronic Health Record. The information in VistA/Patient Electronic Health Record is collected from the individual and first entered in VistA/Electronic Health Record during patient enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares

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.

VA Form 10-10EZ

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.

Prior to any interface implementation a validation plan is designed to assess risk and plan validation requirements to assure the integrity of the data and the interface. Once a connection is successfully made, interface validation commences based on the designed validation plan. All implementation validation plans and the validation itself are signed off the Laboratory Medical Director prior to use in production with patients. Upon sign-off and go-live, the interface integrity is verified regularly (at least once every two years) or whenever a change to the interfaced instrument, interface connection or Instrument Manager Software occurs. In instances where auto verification of results to VistA occur, interface integrity is verified when any of the aforementioned changes occur.

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

The system does not use an external system to check for 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

The SSN is still defined as one of three patient identifiers for positive patient identification (name, full social security number, and date of birth). Properly identified Pathology and Laboratory Medicine patient specimens are critical to veteran care in all clinical settings. Title 38 Section 501 gives authority to collect SSN.

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- System of Record Notice 24VA10A7- Patient Medical Record-VA found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The Path and Lab Med (PALM) System contains sensitive personal information – including social security numbers, names, DOB, ethnicity, and protected health information – of laboratory patient orders that originated in VISTA. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: Veterans Health Administration (VHA) VAEC AWS and PALM as well as the individual facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the VHA. VAEC AWS and PALM security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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.
Patient Name: Used to identify the patient and in other forms of communication
Social Security Number: Used as a patient identifier
Date of Birth: Used to identify age and confirm patient identity
Gender/Sex: Used for gender/sex specific reference range/result reporting
Date of Care: Used to identify the encounter to the patient specimen or order
Visit Date: Used to identify the encounter to the patient specimen or order
Facility Name: Used to route the message appropriately using HL7 standards
Station #: Used to route the message appropriately using HL7 standards

Ward/Room/Bed#: Used for manual result communication, location of patient
Provider Name: Used for result communication
Blood Type: Patient blood typing is performed on some types of laboratory equipment and sent via this middleware to the patient record
Patient Testing Orders and Results: The primary purpose of this system is act as middleware to get Patient Test Orders and Results to/from the patient health record to/from the laboratory medical devices/analyzers
Ordering Provider: The ordering provider is sent with a test order in order to facilitate communication regarding order or associated results
Data File Number (DFN): The laboratory data file number of the patient associated with the order is sent in the order message by the VistA Laboratory Package

The information sent from the VistA Lab Package to the Data Innovations Instrument Manager is in the format of a Test Order. The test order identifies the patient, required demographics for test interpretation and positive patient identification. The test order is then used by the laboratory instruments to run tests as requested by the veteran's healthcare provider. The test result and aforementioned patient information then goes back through the Instrument Manager system software. The software can be configured to manipulate the result data such as applying result flags (high, low, critical low, critical high, etc.) based on patient age, gender or ethnicity, apply reference ranges for result interpretation, order repeat or reflex testing, add interpretive comments to a result, amongst other things based on requirements for best patient care and efficiency. The result information can also be used for business decisions and to assess laboratory workflow efficiencies.

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.

Patient test results, associated flags and reference ranges are sent back through PALM to VistA and stored in the Patient electronic healthcare record for use by the healthcare provider for patient care.

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.

Any data associated with the test result sent from the laboratory medical devices is sent through to VistA to be stored in the Electronic Health Record

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?

PALM receives inheritance from VAEC AWS GovCloud High using VA approved encryption protocols including Virtual Disk and Volume encryption, file folder encryption, Intrusion Detection and Protection Systems (IDPS), Firewall rulesets, endpoint security to scan for malware or other threats to confidentiality and integrity, Physical and logical access control and Change control processes. Application, database and connection safeguards are achieved via self-signed TLS/SSL certificates well as firewall, and Medical Device Isolation Architecture protocols in place for connected medical devices.

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

The above protections (2.3a) are in place to protect SSNs which continue to be the primary patient record number used in the Veterans Health Administration.

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

PII/PHI is protected via PALM System and Communications Protection Standard Operating Procedures. Information is protected information at rest from unauthorized modification or disclosure using FIPS 140-2 encryption

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to the system is maintained via Laboratory Instrument Manager User Access Policy and Procedure.

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

> Access to the system is maintained via Laboratory Instrument Manager User Access Policy and Procedure. System access is maintained by Laboratory Information Managers who have specific training in the use of Instrument Manager software and specifically the User Management Module.

2.4c Does access require manager approval?

System access is maintained by Laboratory Information Managers who have specific training in the use of Instrument Manager software and specifically the User Management Module. Access is role based. Notification of Role is made by the direct supervisor to the Laboratory Information Manager.

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

User Access audits are conducted on a bi-yearly basis by each site Laboratory Information Manager

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

All system users maintain VA Information Security, Privacy and Rules of Behavior training. The VISN 22 Pathology and Laboratory Medicine Service Chiefs assure that all users maintain their Information Security and Privacy training in order to safeguard the PII in PALM.

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*

- Name
- Social Security Number
- Date of Birth
- Associated Laboratory Results

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.*

The data elements included above are retained for 2 years in the Path and Lab Med (PALM).

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

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

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

Yes, the records are maintained in accordance with the records control schedule indicated for the Veterans Medical Record SORN 24VA10A7

There are raw data values from the laboratory analyzers which are maintained for two years

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

In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)

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.

There are no paper documents associated with PALM 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, Electronic Media Sanitization, Directive_6500_24_Feb_2021.pdf When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin.

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.

All IT system and application development and deployment are handled by Enterprise Project Management Office (EPMO). In addition, staff training on functionality in the new or modified application. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. VA Research investigators may use PII for VA Institutional Review Board (IRB)-approved research, and there is no effort to minimize the use of PII for research. Where possible, training and testing occurs in the TEST environment with connectivity is to VistA/CPRS test account. The TEST environment contains no PII.

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.

Follow the format below:

Privacy Risk: There is a risk that the information contained in the Path and Lab Med (PALM) DI IM System will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA Records Administration (NARA). This ensures that data is held for only as long as necessary. To mitigate the risk posed by information retention, the Network 22 VHA Medical Centers adhere to the VARCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center carefully disposes of the data by the determined method as described in question 3. Section 4. Internal Sharing/Receiving/Transmitting and Disclosure. The PALM system has configurable purge settings set to purge records that reach their required retention date.

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***
VistA/CPRS	Laboratory Results from laboratory medical devices for patient care	PHI/PII - Name, SSN, Date of Birth, Ethnicity, laboratory test results	Electronic - TCP/IP HL7
VBECs (VA Blood Bank Electronic Record)	Laboratory Results from laboratory medical devices for patient care	PHI/PII - Name, SSN, Date of Birth, Ethnicity, laboratory test results	Electronic - TCP/IP HL7
Bio-rad SQL Server Instance (OIT)	Quality control data for maintaining laboratory instruments fit for patient testing	Quality Control data points run on laboratory instruments/analyzers – no PHI/PII	Electronic - TCP/IP HL7
Mirth Connect	Business Analytics and advanced procedures not possible within middleware or VistA	Performs advanced procedures not possible within the Hospital or Laboratory Information System or through the Data Innovations middleware product PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen	Electronic – TCP/IP HL7

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. (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 sharing of data is necessary for the medical care of individuals eligible to receive care at a VHA facility. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and response, risk assessment, planning and maintenance.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Role-based assignments are granted by Application Managers. This access is reviewed for appropriateness.

VA Facilities complete a multitude of auditing functions based on VA Handbook 6500 guidelines. VA Facilities complete an in-depth audit of VistA accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as adhoc reports upon request.

The laboratory medical devices reside within an MDIA VLAN to isolate them from other network devices.

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***
NA				

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: The sharing of proficiency data is necessary in order to maintain laboratory accreditation required for operation and patient care. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.
Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, non-persistent, user initiated connectivity, planning and maintenance, rules in place to not allow any PHI or PII to cross via this connection.

All personnel accessing Veteran's information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. A background investigation is required commensurate with the individual's duties.

Individual users are only given job position specific access to individually identifying data. Access to Path and Lab Med (PALM) Accessing requires multi-layer authentication. Path and Lab Med (PALM) Accessing access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts

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 Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP is given out when the Veteran enrolls or when updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior

on an annual basis.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

The Department of Veterans Affairs provides additional notice of this system by publishing System of Record Notice (VHA SORN) Patient Medical Records-VA, SORN 24VA10A7 found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

This Privacy Impact Assessment (PIA) also serves as notice of the Path and Lab Med (PALM) 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.

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

Notice used is that used for enrollment to VistA and follows that adequacy assessment. No one in Pathology or Laboratory Medicine assess adequacy of information collected from veterans at the time of enrollment

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) as well as the VISN 22 facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA.

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VHA permits individuals to agree to the collection 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. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not understand what information is being collected or maintained about them.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. 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.

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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the My HealtheVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. Such as requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

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).

Please provide response here

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.

Please provide response here

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.

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer. Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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.

Right to Request Amendment of Health Information. Veterans have the right to request an amendment (correction) to health information in VHA records if it is believed it is incomplete, inaccurate, untimely, or unrelated to care. Requests must be submitted in writing, specifying the information that to be corrected, and providing a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient information to be amended If request for amendment is denied, the decision will be sent in writing to the veteran and appeal rights provided. In response, the veteran may do any of the following: • File an appeal • File a "Statement of Disagreement" • The veteran may ask that the initial request for amendment accompany all future disclosures of the disputed health information Information can also be obtained by contacting the facility ROI office.

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.

Veterans and individuals should use the formal redress procedures addressed above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veterans receive.

Mitigation: As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records.

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

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

In addition, Privacy and Release of Information Directive 1605.01 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 Path and Lab Med (PALM) is restricted to VA employees from Pathology and Laboratory Medicine Service (PALM), Supporting OIT and Biomedical Engineers with sufficient privileges for access. Specified access is based on the employee's functional category. Role based training is required for individuals with significant administrative and configurations responsibilities.

Access is requested by the Pathology and Laboratory Medicine Server (PALMS) Section Supervisor for PALMS employees based on functional category. Approved access requests initiate account creation by the site Laboratory Information Manager (LIM). VISN 22 Laboratory Information Manager performs bi-annual access audits. Access requests outside of PALMS should be routed through the facility LIM for knowledge and approval.

Two-factor authentication is required for access to the application either via Remote Desktop or via the Thin Client application from Data Innovations for Instrument Manager. Application level access is granted based on the functional category of the user.

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?

No other agencies have access to PALM

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.

Roles include: System Administrator and Application-level access. Application-level access is partitioned based on user role as described above with access managed by Laboratory Information Managers

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.

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the

contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

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 VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to Protected health information or access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused raining. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Review in process
2. *The System Security Plan Status Date:* 7/19/21
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 09/29/22
5. *The Authorization Termination Date:* 03/29/23
6. *The Risk Review Completion Date:* 9/30/22
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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.VA***

Please provide response here

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), 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)*

VA Enterprise Cloud

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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

Please provide response here

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**

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

Signature of Responsible Officials

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.12.12 10:40:18 -08'00'

Privacy Officer, Phillip Cauthers

William Ponce 1698723

Digitally signed by William Ponce 1698723
Date: 2022.12.12 13:37:44 -05'00'

Information System Security Officer, William Ponce

Robin L. Nuspl 124625

Digitally signed by Robin L. Nuspl 124625
Date: 2022.12.12 10:46:28 -08'00'

Information System Owner, Robin Nuspl

APPENDIX A-6.1

Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946