Privacy Impact Assessment for the VA IT System called:

PeriOptimization

Veterans Health Administration (VHA)

Lebanon VA Medical Center

eMASS ID #1229

Date PIA submitted for review:

September 24, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Hromco	Tonya.Hromco@va.gov	717-272-6621 Ext. 4614
Information System Security Officer (ISSO)	Richard Alomar Loubriel	Richard.Alomar-loubriel@va.gov	787-696-4091
Information System Owner	Robert Villare	Robert.Villare@va.gov	717-272-6621, Ext. 3631

Abstract

The abstract provides the simplest explanation for "what does the system do?".

"PeriOptimization" is the name of the system. It is a Perioperative and Procedural services and Dental scheduling and management system. It includes all the clinical forms content from the Computerized Patient Record System (CPRS) in a modified newer technology. It is a scheduling and notification system which documents surgery standard forms and information already used by the Veterans Administration (VA). Example: Name of surgery procedure, laterality, surgeon name. Patient notification on date and time for pre-admission tests and surgery preparation instructions. The Physician is notified if a case is running late—no patient information in the notice. The patient is also notified via text or email if initial procedure time is significantly late (2 hours or more). Vital signs and allergies are also entered. Utilization times are tracked and internally reported as requested by the Lebanon VA Medical Center. It sends text messages with no Personally Identifiable Information (PII) or Protected Health Information (PHI) in the message. At this time text messaging is not being used. This is a future option.

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. What is the IT system name and the name of the program office that owns the IT system?

The IT system name is PeriOptimization, and it is owned by the Lebanon VA Medical Center.

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

The business purpose is to provide a secure scheduling and management system for procedure related services to enhance modernization, efficiency, and safety of Veterans. It is a comprehensive system capable of enterprise use and capable and ready for interoperability and integration with Vista/CPRS consistent with the agency mission.

C. Who is the owner or control of the IT system or project?

VA holds the license to the system. Switchlane owns the product/software and licensed it to the VA.

2. Information Collection and Sharing

D. What is 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 cases is approximately 4750 per year at one facility. A typical client is a Veteran who needs surgery, endoscopy or dental visits and procedures. The total Dental Service visits was approximately 14,000 encounters per year.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The information in the system consists of patient name, last four digits of the social security number (SSN), date of birth (DOB), demographics, procedure date and time, and protected health information (PHI). Additionally, employees, contractors, and clinical trainees' information is also entered into the system. The purpose for collecting this information is to assure accuracy and patient safety for scheduled visits, encounters, and procedures.

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

Information is shared only from the VA corporate data warehouse which is kept behind the VA Firewalls and security intrusion protections. The only items shared are for patient safety and correct identity verification. It is controlled by strict NIST Identity Access Controls and includes the follow items: Age, Allergies, Current medications Date of birth Gender Integrated Control Number (ICN), Last four digits only of the Social Security Number (SSN), Patient Name, Personal Mailing Address, Personal Phone Number, Position Title, Problem List, Procedure, Procedure Date, Vital Signs

G. Is 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?

Currently the system is only utilized at the Lebanon VA Medical Center.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

Patient Medical Record-VA, SORN 24VA10A7. The legal authorities include: Title 38, United States Code, Sections 501(b) and 304 and Title 38, United States Code, Section 501.

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?

The SORN will not need to be modified.

4. System Changes

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

No changes will be required for business process.

K. Will the completion of this PIA could potentially result in technology changes?

No technology changes in the VA systems.

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☐ 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)

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

In addition, the Preoptimization system also collects, uses, disseminates, creates, or maintains the following information:

- Age
- Allergies
- Last four digits of the Social Security Number (SSN)
- Position Title
- Problem List
- Procedure
- Procedure Date
- Vital Signs

PII Mapping of Components (Servers/Database)

PeriOptimization consists of 1 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **PeriOptimization** 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Server 1	Yes	Yes	• Age • Allergies • Current medications • Date of birth • Gender • Integrated Control Number (ICN)	Correct patient identification for patient safety and delivery of appropriate care.	VA firewalls, intrusion protection, PIV and two-factor authentication for access and OS Level Encryption 256k. WASA Scans

			• Last four digits of the Social Security Number (SSN) • Name • Personal Mailing Address • Personal Phone Number • Position Title • Problem List • Procedure • Procedure Date • Vital Signs		

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 system collections information, including contact information, medical history, directly from the individual or from the individual's legal representative. Additional medical information, such has the results of medical appointments, medical tests, prescriptions, and more, are entered into the patient's medical record by facility medical personnel and administrative staff, as appropriate. Providers may refer to the Computerized Patient Record System (CPRS) to confirm patient information. No outside sources are used to obtain information. No financial information is collected.

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.

No source of information outside of CPRS are used or required.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Provides efficiency reports on procedure times. Utilization reports on volume of surgery procedures.

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?

Information is collected directly from patients or information is received via electronic transmission from CPRS. Information is collected during patient interviews, and assessments with the individual. No technologies are used to store or transmit information in identifiable forms. All collected information is used to schedule procedures and/or provide specific services.

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

This system does not collection information on a form.

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.

Information is checked against VistA/CPRS information for accuracy. Information is collected directly from the individual and is assumed accurate. Various staff review data obtained and Health Administration Service staff assist with corrections.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No commercial aggregator is used.

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

•Health Insurance Portability and Accountability Act of 1996 (HIPAA)
•Privacy Act of 1974
•VHA Directive 1605.01 Privacy & Release of Information
•Health Information Technology for Economic and Clinical Health (HITECH) Act
•Patient Medical Records-VA, SORN 24VA10A7
•Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10

From the above SORNs, the legal authorities include: Title 38, United States Code, Sections 501(b) and 304 and Title 38, United States Code, Section 501.

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 PeriOptimization system collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:

The Lebanon VA Medical Center employs a variety of security measures designed to ensure that the information is inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity.

All employees with access to Veteran's health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that 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.

PII/PHI Data Element	Internal Use	External Use
Age	Used as patient demographic, identity, and indicator for type of medical care/provider and medical tests required for individual	Not used
Allergies	Used for history of health care treatment, during treatment and plan of treatment when necessary	Not used
Date of Birth	Used to identify age and confirm patient identity	Not used
Gender	Used as patient demographic, identity, and indicator for type of medical care/provider and medical tests required for individual	Not used
Integrated Control Number (ICN)	Used for accurate patient identification and validation if integrated with VistA/CPRS.	Not Used
Last four digits of the SSN	Used as a patient identifier	Not used
Medications	Used within the medical records for health care purposes/treatment, prescribing	Not used

	medications, and allergy interactions	
Name	Used to identify the patient during appointments and in other forms of communication	Not used
Personal Mailing Address	Used for communication, billing purposes and calculate travel pay	Not used
Personal Phone Number	Used for communication, confirmation of appointments and conduct Telehealth Appointments	Not used
Position Title	Verify employee position title	Not used
Problem List	Used for history of health care treatment, during treatment and plan of treatment when necessary.	Not used
Procedure	Confirm procedure type	Not used
Procedure Date	Confirm procedure date	Not used
Vital Signs	Used for history of health care treatment, during treatment and plan of treatment when necessary	Not used

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?

Only efficiency and operating room utilization reports are provided. No agents, analysts, or outside employees will perform this task.

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.

No new records are created. Any new information is placed into CPRS and not this scheduling system.

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?

Encryption, Web Application Security Assessment (WASA) scans and VA Firewalls, and Personal Identify Verification (PIV) Identity and Access Management (IAM) integration.

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

256k Encryption per National Institute of Standards and Technology (NIST) criteria.

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

All safeguards per VA NIST Cybersecurity is completed and ongoing. Authority to Operate (ATO) via successful security controls implementation.

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?

There are continuous audits of user access to the system. Personal Identify Verification (PIV) integration protects access and use is limited via role permissions consistent with the assigned Functional Categories.

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

Yes

2.4c Does access require manager approval?

Yes, managerial approval is confirmed and required via Security Identification Number or SEC ID for approved users. Every system user must be given a SEC ID which is similar to the PIV Card number assigned for each user. This enables the system to support "two-factor authentication." They must have their PIV Card and enter their unique Code in order to open the system.

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

The system audits user access.

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

OI&T Security assures the safeguards are in place.

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*

Below is the list of information retained by the Perioptimization system as stated in question 1.1.

- Age
- Allergies
- Current medications
- Date of birth
- Gender
- Integrated Control Number (ICN)
- Last four digits of the Social Security Number (SSN)
- Name
- Personal Mailing Address
- Personal Phone Number
- Position Title
- Problem List
- Procedure
- Procedure Date
- Vital Signs

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 the Lebanon VA Medical Center will follow the guidelines established in the VHA Records Control Schedule (RCS) 10-1 and the Office of Information & Technology Records Control Schedule (RCS) 005-1.

All information collected, stored, and used for healthcare and historical information follows the RCS 10-1 for VHA and the RCS 005-1 for Office of Information and Technology retention guidelines, except for, temporary files. Temporary files, also known as working papers, are documents used to make the electronic entries of information or used to temporarily and destroyed when no longer needed by the user.

Medical records are retained for 75 years after the last date of activity. Personnel, administrative, and business records are retained for various amounts of time. The guidance for retention of records is found in the Department of Veterans Affairs, VHA RCS 10-1 and the National Archives and Records Administration.

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

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

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

Yes

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

VHA Records Control Schedule 10-1 (RCS 10-1)
Item number-6000.2
Series-Electronic Health Records (EHR)-Item number 6000.2
Disposition Authority-N1-15-02-3

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.

Information is destroyed by the disposition guidance of the appropriate Records Control Schedule. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this 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. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1 .

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.

PHI/PII may be used for Alpha or Beta testing at the facility-level per VHA policy. Information used solely for training purposes must not contain patient identification. The Lebanon VA Medical Center has test patients (not actual patients) that may be used for the purpose of testing and education. No research is conducted on any information in the system.

VHA must minimize the use of PHI and PII in training presentations or materials per VA policy. Any presentations that contain information based on patients must be routed through the Facility Privacy Officer to ensure all 18 HIPAA identifiers have been removed.

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 maintained in the system could 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, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, the Lebanon VA Medical Center adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The Lebanon VA Medical Center ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using, and retaining this data. A Facility Records Officers, Privacy Officer, and an Information System Security Officer are assigned to each VA Medical Center to ensure their respective programs are understood and followed by all to protect sensitive information from the time the VA captures it until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and to assist staff with questions concerning the proper handling of information.

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 Information Systems and Technology Architecture (VistA)	Purpose is for accuracy, avoid human entry errors and safety	• Age • Allergies • Current medications • Date of birth • Gender • Integrated Control Number (ICN) • Last four digits of the Social Security Number (SSN) • Name • Personal Mailing Address • Personal Phone Number • Position Title • Problem List • Procedure • Procedure Date • Vital Signs	Electronically, Computer Local Area Network (LAN)

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 the appropriate surgical care at the Lebanon VA Medical Center. 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

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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 Lebanon VA Medical Center provides notice of information collection in several additional ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA System of Record Notices (VA SORN) in the Federal Register and online.

- Patient Medical Records-VA, SORN 24VA10A7
- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10
- https://department.va.gov/privacy/system-of-records-notices/
- This Privacy Impact Assessment (PIA) also serves as notice of the Perioptimization system. 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."
- VHA Notice of Privacy Practices
- VHA Handbook 1605.04: Notice of Privacy Practices

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

VHA Notice of Privacy Practices

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 interacting with VA. The NOPP is mailed to all enrolled Veterans every three years or when there is a major change.

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

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

Yes, individuals do have an opportunity to decline to provide information at any time. However, if the information is not furnished completely and accurately the VA may be unable to comply with the request. The VHA may not condition treatment, payment, enrollment, or eligibility on signing an authorization.

The Notice of Privacy Practices states that the Veteran has the right to request a restriction of the use and disclosure of information; however, under 45 CFR § 164.522(a)(1)(vi) the VHA is not required to agree to such a restriction. Employees and VA contractors are also required to provide requested information to maintain employment or contracts with the Lebanon VA Medical Center.

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.

The Lebanon VA Medical Center allows individuals to agree to the collection of their PHI/PII by using 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 employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including the Privacy Act Statements on forms collecting personal information from Veterans or individuals.

The Lebanon VA Medical uses PHI/PII only as legally permitted including obtaining authorizations when required. When there is no legal authority to disclose information, the Lebanon VA Medical Center obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PHI/PII. Individuals have the right to consent to use of U.S.C. 7332 (Alcohol and Substance Abuse, HIV, and Sickle Cell Anemia) and medical records by completing VA Form 10-5345.

Individuals have a right to restrict the disclosure and use of their health information by submitting a written request to the facility Privacy Officer where they are receiving their care.

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:

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

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

Privacy Risk: There is a risk that Veterans and other members of the public will not know that the PeriOptimization system exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them. Most patients are aware that information regarding their procedures is kept on electronic information systems inside the VA.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. 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 (SOR) 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 follow procedures to gain access to their information under the guidelines of the Privacy Act, Freedom of Information Act (FOIA), and Health Insurance Portability and Accountability Act (HIPAA).

Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the Lebanon VA Medical Center. When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own

Health Information, which can be obtained from the Lebanon VA Medical Center Release of Information Office.

Additionally, Veterans can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealthevet program, VA's online personal health record. More information about MyHealthevet can be found at https://www.myhealth.va.gov/index.html.

In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at https://department.va.gov/privacy/system-of-records-notices/

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)?

The system is not exempt from the access provisions of the Privacy Act.

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?

This is a Privacy Act system. Therefore, an individual can access their information as stated above.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are 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 SOR. Every Privacy Act SOR contains 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.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary. Individuals have the right to review and change their contact or demographic information at the time of appointment or upon arrival to the VA facility.

If corrections are needed to a legal name, date of birth, or social security number, the Centralized Business Office (CBO) or other staff as applicable, would process the request requiring a valid driver's license, state identification, passport, military ID, or a letter from the Social Security Administration in addition to a signed amendment request from the individual requesting the change. The signed amendment request and legal documentation is then sent to the Privacy Officer for processing.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The Notice of Privacy Practices explains an individual's right to request an amendment (correction) to their health information if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. Information can also be obtained by contacting the facility Release of Information Office or Privacy Office.

Lebanon VA Medical staff and providers are educated to refer the individual to the Privacy Office for requests to amend (correct) their record.

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.

Redress is provided through the Privacy Act for the individual to view and request correction their information. If the request is denied, the individual can appeal the decision by writing to the Office of General Counsel (024); Department of Veterans Affairs; 810 Vermont Avenue, N.W.; Washington, D.C. 20420.

The Privacy Act and HIPAA permit the individual to also complete a Statement of Disagreement to the information that was denied a correction. The facility may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the facility Privacy Officer, must provide a copy to the individual. The individual's request for an amendment, the facility's denial of the request, the individual's statement of disagreement, if any, and facility's rebuttal, if prepared, must be appended or otherwise linked to the individual's record.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs***

to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The Lebanon VA Medical Center 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.

As discussed in question 7.3, Veterans received the NOPP every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records.

The Lebanon VA Medical Center Release of Information (ROI) office is available to assist Veterans with obtaining access to their health 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 and have access to the premium account 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?

Individuals receive access to the PeriOptimization system by gainful employment in the VA or upon being awarded a contract that requires access to the system. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. User access to the system requires issuance of a PIV card and all the security that entails. Then users must be given a special SEC ID to access the PeriOptimization system which is IAM and PIV integrated.

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 agency may access this system.

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.

Read/view access is only given to some staff such as sterilization staff to determine the number of sterile carts needed for the next day's surgery. There is an administrative role for elevated permissions to enable user access, but they have no clinical permission. Physician, nursing, and scheduler roles are based on assigned functional categories and a need to access the system.

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.

Contractors will only have access to the PeriOptimization system on a need-to-know basis in the performance of their contracted assignments/task. VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete job duties as stated within the contract. Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).

Per specific contract guidelines, contractors can have access to the system only after completing mandatory VA Privacy and Information Security Awareness and Rules of Behavior training, Privacy and HIPAA Focused training and the appropriate background investigation to include fingerprinting. Certification that all contractors have completed this training must be provided to the VHA employee who is responsible for the contract (e.g., COR) if the training is not completed in Talent Management System.

All contracts that do not involve treatment of an individual by which contractors may need access to PHI/PII 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 Area Lebanon personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the Area Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained.
The Talent Management System offers the following applicable privacy courses:

VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPAA Training Focused Training
VA 3185966: VHA Mandatory Training for Health Professions Trainees (HPTs)
VA 3192008: VHA Mandatory Training for Health Professions Trainees (HPTs-Refresher)
VA 20152: Mandatory Training for Transitory, Part-time and Intermittent Clinical Staff

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

8.4a If yes, provide:

1. *The Security Plan Status:* Current & Approved
2. *The System Security Plan Status Date:* 08 December 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11 August 2023
5. *The Authorization Termination Date:* 10 August 2025
6. *The Risk Review Completion Date:* 15 May 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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 cloud technology used at present. The system will utilize VA Enterprise Cloud (VAEC) next year.

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.*

No Cloud Presence at this moment.

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

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

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

No cloud presence at this moment.

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.

We are not in the cloud. Not applicable.

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

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

Not in the cloud. Not Applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
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.

TONYA HROMCO

Digitally signed by TONYA HROMCO
Date: 2024.10.08 12:45:51 -04'00'

Privacy Officer, Tonya Hromco

RICHARD ALOMAR-LOUBRIEL

Digitally signed by RICHARD ALOMAR-LOUBRIEL
Date: 2024.10.09 13:04:28 -04'00'

Information System Security Officer, Richard Alomar Loubriel

ROBERT VILLARE

Digitally signed by ROBERT VILLARE
Date: 2024.10.09 11:32:29 -04'00'

Information System Owner, Robert Villare

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; screen shot of a website collection privacy notice).

https://department.va.gov/privacy/system-of-records-notices/

Patient Medical Records-VA, SORN 24VA10A7

Veterans Health Information Systems and Technology Architecture (VistA) Records VA, SORN 79VA10

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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