Privacy Impact Assessment for the VA IT System called:

# VAPALS-ELCAP Lung Cancer Screening Management System

# Veterans' Health Administration (VHA)

# Office of Healthcare Innovation and Learning (OHIL)

# eMASS ID #1445

Date PIA submitted for review:

12/19/2023

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nancy Katz-johnson | Nancy.katz-johnson@va.gov | 203-535-7280 |
| Information System Security Officer (ISSO) | Jerome Rabanal | jerome.rabanal@va.gov | 858-642-1533 |
| Information System Owner | Angela Gant-Curtis | Angela.gant-curtis@va.gov | (540) 760-7222 |

## Abstract

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

VAPALS-ELCAP (Veterans Affairs Partnership to increase Access to Lung Screening – Early Lung Cancer Action Program) Lung Cancer Screening Management System is a Veterans Information Systems and Technology Architecture (VistA) based system that provides VA clinicians a web interface for tracking and managing lung cancer screening services for Veterans. If a Veteran chooses to enroll in a VA medical center's lung cancer screening program, a clinician user enters patient information into the system to register the Veteran for multi-year tracking. Once a Veteran is registered, the system generates an intake note for Computerized Patient Record System (CPRS) and creates a care path. Radiologists use the software to document findings seen on lung cancer screening computed tomography (CT) scans. The software generates a radiology report that is copied and pasted into the radiology computer system (for example, picture archiving and communication system, PACS); from there, a report is sent to CPRS through already established channels. Clinicians will use the VAPALS-ELCAP software for overall program management of the VA medical center's lung cancer screening program, as well as management of individual Veteran services. The software generates summary reports for the program staff to monitor and manage quality and safety. Health Level 7 (HL7) bridges will allow two-way communication between the VAPALS-ELCAP system and CPRS. This is a minor application associated w/the eScreening (MHE) (Cloud) Assessing system hosted within VA Enterprise Cloud (VAEC): Amazon Web Services (AWS).

## 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 VAPALS-ELCAP (VA Partnership to increase Access to Lung Screening – Early Lung Cancer Action Program) Lung Cancer Screening Management System is owned by the VA-PALS program office and sponsored by the Veterans Health Administration (VHA) Office of Specialty Care Services for Office of Healthcare Innovation and Learning (OHIL).

*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 purpose of VAPALS-ELCAP is to aid clinicians in tracking and managing lung cancer screening programs at VA medical centers. The web-based interface has structured forms in which VA clinicians document Veterans' enrollment in a lung cancer screening program and enter the results of their radiology scans and any resulting follow-up procedures. The VAPALS-ELCAP software communicates bidirectionally with Enterprise VistA such that documentation entered into the web-based forms is added as a

note in the patient's medical record. Clinicians use VAPALS-ELCAP to run program management reports that, for example, list patients who are due for a screening CT scan or a follow-up procedure. These management reports help local program coordinators to ensure timely transitions between screening, follow-up procedures, cancer diagnosis, and cancer care. These functionalities support VHA's mission by improving the effectiveness, quality, and safety of lung screening programs which are currently serving thousands of VHA enrollees.

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

A Class I version of VAPALS-ELCAP is currently running at the Phoenix VA Medical Center under a local ATO boundary. Once hosted in the VAEC-AWS environment, all VA facilities will be able to utilize the system. Authority to Operate: Title 38 of U.S Code section 201. VistA, 79VA10.

*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 system stores information for VHA patients who have been referred to or have enrolled in a VA medical center's lung cancer screening program. The expected number of Veterans whose information will ultimately be stored in the system is about 30,000.

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

Information gathered and stored in this system include the Veteran's name, social security number, date of birth, mailing address, phone number, presenting health issues/symptoms, diagnosis codes, Health Factors, and radiology reports. Information is sent from Enterprise VistA to VAPALSELCAP in Orders and in Text Integration Utility (TIU) notes that are communicated bidirectionally via HL7 interfaces.

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

VAPALS-ELCAP communicates with the EHR using HL7. When a veteran is enrolled in the lung screening program, an order is placed in VistA; this order provides the veteran's information to the VAPALS-ELCAP system. The VAPALS-ELCAP system sends a text note back to VistA via HL7 that summarizes the intake data entered for the veteran.

*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?*

The system will be available for use by multiple VA medical centers. Use of the system and PII/PHI will be maintained consistently in all sites through supervision by the system administrator and training provided to all users by the VA-PALS program office. The same security controls are addressed by the eScreening (MHE) (Cloud) system which is the major application under which VAPALS-ELCAP is a minor application. The same security controls will be used across all sites.

*3. Legal Authority and SORN*

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

Privacy Service has determined the Privacy Act of 1974, 5 U.S.C. § 552a (e), Section 208(c), E-Government Act of 2002 (P.L. 107-347), and the Office of Management and Budget (OMB)Circular A-130,

Appendix I are the legal authority to permit the collection, use, maintenance and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. The Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs): 1) The VHA SORN Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf). 2) The VHA SORN Veterans Health Information Systems and Technology Architecture (VistA)Records-VA, SORN 79VA10 (Dec. 23, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf).Enterprise VistA, and all VHA facilities' VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a). Additionally, 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), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).Additional information about state laws, local policies, and more can be found by reviewing the individual facility Privacy Impact Assessments (PIAs). https://www.oprm.va.gov/privacy/pia.aspx.

*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?*

There are no system of records notice (SORN) modifications or approvals needed. The Department of Veterans Affairs maintains ownership and rights over all data. The VA Enterprise Cloud contract includes language and processes for security and privacy of data. VAPALS-ELCAP is a minor application under the major application eScreening (MHE) (Cloud) which is categorized as a MODERATE impact system.

*4. System Changes*

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

The completion of the PIA will not result in circumstances that require changes to the business process.

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

Completion of this PIA will not result in technology changes.

## 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)

Other PII/PHI data elements: Additional information collected: Age, Marital status, presenting health issues, symptoms, diagnosis codes, Health Factors, radiology reports, and other clinical data pertaining to tobacco use and lung cancer screening, and employee VistA ID.

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

**PII Mapping of Components (Servers/Database)**

**VAPALS-ELCAP Lung Cancer Screening Management System** consists of one key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VAPALS-ELCAP Lung Cancer Screening Management System** 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 |
|---|---|---|---|---|---|
| Enterprise VistA - Cache | **Yes** | **Yes** | Full Name, Personal mailing address, age, sex, race, marital status, phone number, date of birth, SSN, Medical Record Number, diagnosis codes, Health Factors, radiology reports, presenting health issues, symptoms, diagnosis | Name, age, gender, DOB, and SSN are collected/stored for the purpose of identifying patients. Phone number and mailing address are collected/stored for providers to use when contacting patients. PHI is used to create care plans for individuals and to manage the provision of lung cancer screening and treatment | Hosted in private VA Enterprise Cloud (Amazon Web Services), controlled physical and logical access, only approved and authorized users granted access to application. |

| | | | | | |
|---|---|---|---|---|---|
| | | | codes, and other clinical data related to tobacco use and lung cancer screening. | | |

**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?*
Information is collected directly from the Veteran during encounters with clinicians associated with the VA medical center's lung screening program. Information is also collected from the Veteran's electronic medical record in Enterprise VistA (Veterans Health Information Systems and Technology Architecture) in the form of Orders.

*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 lung screening program staff or other health care provider completes standardized forms for intake encounters and follow-up encounters with the Veteran regarding their participation in the lung screening program.

*1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?*
Upon completion of a standardize forms in the VAPALS-ELCAP system, a Text Integration Utility (TIU) note with the text of the form is sent via Health Level 7 (HL7) to the Veteran's electronic medical record in Enterprise VistA. The radiologist completes a standardized form with their interpretation of low-dose CT scans. Completion of this form generates text which the radiologist copies and pastes into the radiology software suite (for example, picture archiving and communication system, PACS). Then, this radiology report is sent from the radiology software suite to the Veteran's electronic medical record in Enterprise VistA

**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 in three ways: 1. Information is collected verbally from the Veteran during interviews and conversations with VA medical staff, who enter this information into structured forms in the VAPALS-ELCAP web interface. 2.VA radiologists enter clinical information about the Veteran's CT scans into structured forms in the VAPALS-ELCAP web interface, and other VA providers record the Veteran's laboratory or intervention results into structured forms in the VAPALS-ELCAP web interface. 3.VAPALS-ELCAP retrieves demographic and clinical information from Enterprise VistA via Orders transmitted by HL7.

*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?*

VAPALS-ELCAP is not subjected to Paperwork Reduction Act.

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

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

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

All data transmissions occur within the VA firewall via HL7. Information that is transmitted electronically from Enterprise VistA to the VAPALS-ELCAP server will be assumed to be accurate. Information obtained directly from the Veteran will be assumed to be accurate. Information entered into VAPALS-ELCAP by the VA clinician will be assumed to be accurate.

*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?*

Each VA clinician-user of VAPALS-ELCAP will receive role-based training by the VA-PALS program office to ensure accuracy. Patient demographic data is automatically updated, if necessary, when any new Order is sent from Enterprise VistA. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Please review the individual PIAs for facility specific information about information accuracy. https://www.privacy.va.gov/privacy_impact_assessment.asp

**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*

VA Privacy Service has determined the Privacy Act of 1974, 5 U.S.C. § 552a (e), Section 208(c), E-Government Act of 2002 (P.L. 107-347), and the Office of Management and Budget (OMB)Circular A-130, Appendix I are the legal authority to permit the collection, use, maintenance and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. The Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs): 1) The VHA SORN Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf). 2) The VHA SORN Veterans Health Information Systems and Technology Architecture (VistA)Records-VA, SORN 79VA10 (Dec. 23, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf).Enterprise VistA, and all VHA facilities' VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a).Additionally, 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), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).Additional information about state laws, local policies, and more can be found by reviewing the individual facility Privacy Impact Assessments (PIAs). https://www.oprm.va.gov/privacy/pia.aspx

### 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 VAPALS-ELCAP System contains sensitive personal information – including social security numbers, names, and protected health information on Veterans. 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:** VAPALS-ELCAP, VHA, Enterprise VistA, VA Enterprise Cloud, and the VHA 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. 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 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 |
|---|---|---|
| Name | File Identification purposes | Not used |
| Social Security Number | File Identification purposes | Not used |
| Date of Birth | File Identification purposes | Not used |
| Personal Phone | File Identification purposes | Not used |
| Medical Record Number | File Identification purposes | Not used |
| Gender | File Identification purposes | Not used |
| Age | Diagnosis | Not used |
| Race | File Identification purpose | Not used |
| Marital Status | File Identification purposes | Not used |
| Presenting Health issues | Diagnosis | Not used |
| Symptoms | Diagnosis | Not used |
| Diagnostic Codes | Diagnosis | Not used |
| Health Factors | Diagnosis | Not used |
| Radiology Reports | Diagnosis | Not used |
| Tobacco Use | Diagnosis | Not used |
| VistA ID | File Identification purposes | 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?*
When registering a Veteran in the VA medical center's lung cancer screening program, the VA clinician will ask the Veteran questions about their tobacco use and lung health and enter the Veteran's responses into structured forms. Other structured forms will be used to document the results of lung cancer screening CT (computed tomography) scans, document communications between the lung cancer screening program and the Veteran, and document follow-up procedures. When a structured form is completed by the VA provider in the system's web interface, a TIU (text integration utility) note will be inserted into the Veteran's medical record in Enterprise VistA.

*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.*

Some analysis may be conducted on aggregate patient data for quality control purposes, but no results of this analysis will be relevant or included in individual Veteran records and will only be used for quality control purpose.

### 2.3 How is the information in the system secured?

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

*2.3a What measures are in place to protect data in transit and at rest?*
Data stored in the VAPALS-ELCAP database, exchanged point-to-point over the VA network between VistA and VAPALS-ELCAP, displayed to users (VA employees) in our VAPALS-ELCAP web user interface, and exchanged point-to-point (encrypted via https) between VAPALS-ELCAP and the user's browser.

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

SSNs are shown in partial form, available to certain approved VAMC users. This system is a customized VAPALS-ELCAP instance of VistA, therefore SSNs are protected in the same way that they are protected in any current VistA production environment. Patient SSN is stored in the VAPALS-ELCAP database, exchanged point-to-point over the VA network between VistA and VAPALS-ELCAP, displayed to users (VA employees) in our VAPALS-ELCAP web user interface, and exchanged point-to-point (encrypted via https) between VAPALS-ELCAP and the user's browser.

*2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?*
PII/PHI is safeguarded through limited user access by role/function and managed by the technical controls as outlined in VA HANDBOOK 6500.

**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 PII is limited to appropriate individuals for whom the system administrator has created a user account. Individuals must have a VistA account in order to receive an account with this system.

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

The VAPALS-ELCAP system administrator is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual and technical manual.

*2.4c Does access require manager approval?*

Yes

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

The system administrator monitors, tracks, and records all users' access to the VAPALS-ELCAP application and the PII stored in the application. All system users are trained in how to appropriately use patient information for the performance of their clinical duties. If an individual is found to be inappropriately using information, the system administrator will revoke that individual's user account.

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

The VAPALS-ELCAP system administrator is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual and technical manual.

## 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*

The system retains the following types of PII: Name, age, gender, DOB, SSN, phone number, and mailing address. The system retains the following types of PHI: Diagnosis codes, Health Factors, radiology reports, presenting health problems, symptoms, and other clinical data pertaining to tobacco use and lung cancer screening.

**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.*

Records generated in the VAPALS-ELCAP system and stored in Enterprise VistA have a 75-year retention period after a Veteran's last episode of care in a VA health care facility. Data stored in the VAPALS-ELCAP system itself will follow the same record retention schedule.

**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?*

Records generated in the VAPALS-ELCAP system and stored in Enterprise VistA will follow the retention schedule described in the NARA-approved Department of Veterans Affairs Record Control Schedule (RCS)-10, Chapter 6 Healthcare Records, Item No. 6000.1 (January 2020; https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf):Health Records Folder File or CHR

(Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. Records stored in the VAPALS-ELCAP system itself will apply the above record retention schedule as follows: Patient records will be retained for a total of 75 years after the Veteran's last episode of care that is recorded in the VAPALS-ELCAP system.

**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.*

For records generated in the VAPALS-ELCAP system and stored in Enterprise VistA, electronic data and files of any type, including Protected Health Information (PHI) and Sensitive Personal Information (SPI), are destroyed in accordance with the VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev 1, Guidelines for Media Sanitization (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf) and the VA Media Sanitization User's Guide (November 17, 2014). When required, these data are deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Additionally, each VHA facility follows FSS Bulletin #209.1 National Media Sanitization and Destruction Program, as well as OIT-OIS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization. For records stored in the VAPALS-ELCAP system itself, electronic data and files of any type, including Protected Health Information (PHI) and Sensitive Personal Information (SPI), are destroyed by deletion 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.*

In non-production environments, no PII or actual patient/user information is used for simulating specific transactions in the application. "Synthetic" patient information is used in testing and development. This faux data is created using an algorithm created by Mitre. Some test patient data is also created by developers to test certain edge cases. Production should be the only environment to contain actual patient data.

**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:** Any time data is retained there is a risk that records may be unintentionally released or breached**.**

**Mitigation:** VAPALS-ELCAP data is only stored within VA networks. No data is allowed to be moved outside of VA control. Rules for retention and disposition of data housed for VAPALS-ELCAP is based on standards developed by the National Archives Records Administration (NARA). Security measures required by VA policy and NARA are scrupulously followed in VAPALS-ELCAP development and processes.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

**4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

**NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Veterans Health Administration Enterprise VistA | Information is collected from and shared with Enterprise VistA for the purpose of planning and managing the provision of health care services. | Enterprise VistA will transmit demographic data (Name, SSN, DOB) to the system. The system will transmit clinical data (Presenting health issues, Health Factors, radiology reports, diagnosis codes) to Enterprise VistA in the form of clinical care notes (Text integration utility, TIU notes). | Information is electronically received from and transmitted to Enterprise VistA via HL7 on the secure VA network (using CPRS to interface with Enterprise VistA using HL7). |

### 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 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 entity 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 environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

## 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*** | ***List the purpose of information*** | ***List the specific PII/PHI data elements that are processed*** | ***List the legal authority,*** | ***List the method of transmission*** |
|---|---|---|---|---|

| ***information is shared/received with*** | ***being shared / received / transmitted with the specified program office or IT system*** | ***(shared/received/transmitted)with the Program or IT system*** | ***binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*** | ***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 externa, sharing.

**Mitigation:** There is no externa, 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 VHA Notice of Privacy Practice (NOPP)**
**https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946**
**explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.**

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

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

**Notice is also provided in the Federal Register with the publication of the SORN:**
*provide the citation.*

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

The VHA SORN Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020), in the Federal Register and online

*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 Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs):1)The VHA SORN Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf).2)The VHA SORN Veterans Health Information Systems and Technology Architecture (VistA)Records-VA, SORN 79VA10 (Dec. 23, 2020), in the Federal Register and online (https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf).

**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 VAPALS-ELCAP program requests only information necessary to provide services to Veterans at VHA facilities. While a Veteran may decline to provide information to the program, this may prevent the Veteran from participating in the VA medical center's lung cancer screening program, depending on which information the Veteran declines to provide.

**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.*

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing.

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

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

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

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

*<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*
Follow the format below:

**Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

**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 at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also 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.***

Notes and reports are sent to and filed in the facility's VistA system where they can be accessed by the Veteran in MyHealtheVet in the same way other records can be accessed. Veterans may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

*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?*

The system is a Privacy Act system.

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

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

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from their facility's Release of Information (ROI) office. The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writes 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.

**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.*

VAPALS-ELCAP relies on the Notice of Privacy Practice (NOPP) process, which states: Right to Request Amendment of Health Information: You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: •File an appeal •File a "Statement of Disagreement" •Ask that your initial request for amendment accompany all future disclosures of the disputed health information. Information can also be obtained by contacting the 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 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 affect the care the Veteran receives.

**Mitigation:** As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every Veteran receives when they enroll, discusses the process for requesting an amendment to their records.
The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans Health Administration (VHA) established the MyHealtheVet 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?*
VA employees, who must complete both the HIPAA and Information Security training, are granted access to VAPALS-ELCAP based on the employee's functional category. Role-based training is required through the VA-PALS program office. VA employees request access to VAPALS-ELCAP when the user's supervisor emails the VAPALS-ELCAP system administrator to request the creation of a user account. Users submit access requests based on need to know and job duties.

*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 external users from other agencies will have access to the 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.*
VA clinicians involved in lung cancer screening, diagnosis, and treatment will be authorized to access, create, and make changes to the information about patients who they treat at their VA facility, but will not be authorized to access information about patients who do not receive care at the clinician's VA facility.

**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.*
Currently, one individual contractor will have access to the system for system maintenance and emergency purposes in the event of a system crash or the need for system maintenance when the usual system administrator (a VA employee) is not available. Other contractors, who develop the software, do not have access to the VAPALS-ELCAP production system or any patient information. All regularly scheduled maintenance and work is performed by VA employees. Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., Contracting Office Representative, Contracting Officer, Contract Review Committee).Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA (HIPAA) Health Insurance Portability and Accountability 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 in the contract clarification of the mandatory nature

of the training and the potential penalties for violating patient privacy. Contractors must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees. All contractors are required to sign a mandatory non-disclosure agreement (NDA) before accessing VA systems or data. The system contacts for VAPALS-ELCAP will provide a copy of the NDA upon request.

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

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

All users will be VA employees with active VistA accounts. 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 PHI or access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused training. 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 presents subject specific training 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:* Approved
2. *The System Security Plan Status Date:* 12/08/2023
3. *The Authorization Status:* Assessment Approved
4. *The Authorization Date:* 05/19/2023
5. *The Authorization Termination Date:* 05/19/2024
6. *The Risk Review Completion Date:* 05/19/2023
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.***

<VAPALS-ELCAP is a minor application covered under the active ATO boundary of the eScreening (MHE) (Cloud) Assessing system, which is hosted within VAEC-AWS and classified as a MODERATE impact system. The Minor Application Self-Assessment for VAPALS-ELCAP is in process. The IOC date for VAPALS-ELCAP is 5/1/2021.

## 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)*

The system is *Infrastructure as a Service (IaaS),* VAEC

**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.*

<<ADD ANSWER 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.*

<<ADD ANSWER 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.*

<<ADD ANSWER 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).*

<<ADD ANSWER 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** |
| 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.**

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.02.21 15:57:53 -05'00'

**Privacy Officer, Nancy Katz-johnson**

JEROME RABANAL

Digitally signed by JEROME RABANAL
Date: 2024.02.21 07:38:13 -08'00'

**Information System Security Officer, Jerome Rabanal**

ANGELA GANT-CURTIS

Digitally signed by ANGELA GANT-CURTIS
Date: 2024.02.20 21:34:18 -06'00'

**Information System Owner, Angela Gant-Curtis**

## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

## 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