Privacy Impact Assessment for the VA IT System called:

Capacity & Performance Engineering

VACO

Office of Information and Technology (OIT), Development, Security, and Operations (DevSecOps), Product Engineering (PE), Capacity and Performance Engineering (CPE)

Date PIA submitted for review:

August 25,2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Craig Heitz	Craig.Heitz@va.gov	612-724-2132
Information System Owner	Tony Lengvinis	Tony.Lengvinis@va.gov	203-887-7241

Abstract

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

The Capacity & Performance Engineering (CPE) is a testing lab used by Software Product Management (SPM), to support capacity and performance testing for large applications (HealtheVet, Legacy VistA, and WAN emulation testing).The test lab supports HealtheVet (over 47 application systems), Legacy VistA, and WAN emulation testing. This effort creates a "data center island" in the computer room that mimics the production environment of each of these systems, because actual patient data including Protected Health Information (PHI) and Personally Identifiable Information (PII) resides on CPE test systems.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

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

Please provide response here

Capacity & Performance Engineering (CPE) and Owned by OI&T/SPM/Health Services/VERDI/CPE, located in Austin Information Technology Center (AITC)

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

CPE pre-production VistA is a development environment designed to provide developers a production-like environment for testing new software releases prior to release to production systems.

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

CPE pre-production VistA is administered and maintained by Capacity and Performance Engineering (CPE), which resides within Software Production Management's (SPM) Health Services.

2. Information Collection and Sharing

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

The CPE pre-production VistA systems uses copies of production VistA system databases. Each CPE database entry represents a copy of a VA patient record from a production electronic medical record. In aggregate, there are approximately 1,099,009 patient records copied from the Boston, Central Texas, Cheyenne, Dayton and Muskogee production VistA systems.

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

The CPE system contains copies of production patient records from multiple VA healthcare facilities' VistA electronic medical record systems. No data is directly collected from VA patients, rather, production data is copied into this system.

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

The CPE system shares specific data elements with other internal VA systems as part of an integrated system of systems electronic health record. The intent is not to provide medical data for healthcare providers, rather, it is to provide a replica of production system interactions so that developers can test code in a production-like environment prior to release.

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

The CPE systems is operated solely at the Austin Information Technology Center.

3. Legal Authority and SORN

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

SORN 121VA10 / 88 FR 22112 National Patient Databases-VA and 79VA10
85 FR 84114 Veterans' Health Information Systems and Technology Architecture (VistA) Records-VA

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

N/A

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers

☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

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

PII Mapping of Components (Servers/Database)

Capacity & Performance Engineering consists of **28** 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 **Capacity & Performance Engineering** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
oitetndhcdvxpca/ xpcr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Previous Medical Records, Race/Ethnicity, Financial Account Information.		
oitetndhcdvxpcb/ xpcr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxpba/ xpbr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis;	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	system modeling and planning.	
oitetndhcdvxpbb/ xpbr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxpta/ xptr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone	The stored PII is used to emulate a production VistA environment for purposes of: development	CPE protects the confidentiality, integrity and availability of information through privacy and security

			Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	and testing of new software and systems; root cause analysis; system modeling and planning.	controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxptb/ xptr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxpda/ xpdr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA	**Yes**	Name, Social Security Number, Date of Birth,	The stored PII is used to emulate a production	CPE protects the confidentiality, integrity and

	does store PII previously collected by the source IT system		Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxpdb/ xpdr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Account Information.		
oitetndhcdvxpma/ xpmr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxpmb/ xpmr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Previous Medical Records, Race/Ethnicity, Financial Account Information.		
oitetndhcdvxdb/ xdbr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxdc/ xdcr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis;	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	system modeling and planning.	
oitetndhcdvxdd/ xddr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxdl/ xdlr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone	The stored PII is used to emulate a production VistA environment for purposes of: development	CPE protects the confidentiality, integrity and availability of information through privacy and security

			Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	and testing of new software and systems; root cause analysis; system modeling and planning.	controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdvxdt/ xdtr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcavxpb/ xpbr8ta01	No – CPE VistA does not directly collect PII. CPE VistA	**Yes**	Name, Social Security Number, Date of Birth,	The stored PII is used to emulate a production	CPE protects the confidentiality, integrity and

	does store PII previously collected by the source IT system		Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcavxpc/ xpcr8ta01	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Account Information.		
oitetndhcavxpd/ xpdr8ta01	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcavxpt/ xptr8ta01	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Previous Medical Records, Race/Ethnicity, Financial Account Information.		
oitetndhcavxpm/ xpmr8ta01	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv501/ xmtr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis;	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	system modeling and planning.	
oitetndhcdv502/ xmbr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv503/ xmcr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone	The stored PII is used to emulate a production VistA environment for purposes of: development	CPE protects the confidentiality, integrity and availability of information through privacy and security

			Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	and testing of new software and systems; root cause analysis; system modeling and planning.	controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv504/ xmdr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv505/ xmmr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA	**Yes**	Name, Social Security Number, Date of Birth,	The stored PII is used to emulate a production	CPE protects the confidentiality, integrity and

	does store PII previously collected by the source IT system		Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv506/ xmpr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Account Information.		
oitetndhcdv507/ xmvr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB
oitetndhcdv508/ xmlr8tsvr	No – CPE VistA does not directly collect PII. CPE VistA does store PII previously collected by the source IT system	**Yes**	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication,	The stored PII is used to emulate a production VistA environment for purposes of: development and testing of new software and systems; root cause analysis; system modeling and planning.	CPE protects the confidentiality, integrity and availability of information through privacy and security controls implemented in GRC Risk Vision and VA 6500HB

			Previous Medical Records, Race/Ethnicity, Financial Account Information.		

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 from the source production IT systems by electronic file transfer. HealtheVet, Legacy VistA; the test lab supports HealtheVet (over 47 application systems), Legacy VistA, and WAN emulation testing. This effort will create a "data center island" in the computer room that mimics the production environment of each of these systems. The VistA Kernel software provides identification and authentication, access control via menu management, and auditing of user actions. VA FileMan, VistA's database management software, in conjunction with the Kernel, provides data access control

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 system is a replica of production VistA systems. As such it uses copies of actual production data from the actual production systems.

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

The system does not create new information. There is no "new" data added to an individual patient record.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

All information in CPE PreProduction VistA is electronically transferred securely from other VA source systems such as HealtheVet (over 47 application systems), Legacy VistA and VA Wide Area Network (WAN).

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

Please provide response here
N/A, no paper collection of information is done.

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.

-
- Individual data elements are not validated for accuracy. Rather, CPE depends on the source production systems to perform whatever data validation they deem important. As the data within the CPE lab systems are not used for their original intended purposes, e.g. healthcare, data accuracy is not critical.

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

CPE focuses on accuracy of system modeling. System model accuracy is determined by comparing production system design parameters and performance metrics against those of the lab system under study. Commercial data aggregator is not utilized.

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

- Records are retrieved by name, social security number or other assigned identifiers of the individual on whom they are maintained. Title 38, United States Code, Section 501 is the authority for maintaining the system stated in the System of Record Notice (SORN) 121VA10 / 88 FR 22112 - National Patient Databases-VA and 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

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: CPE PreProduction VistA stores previously collected Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to complete the mission of the business/service line components. By only collecting

the minimum necessary information, the VA is able to better protect the individual's information. CPE PreProduction VistA is a pre-production platform for testing various changes to several systems and applications. Information is gathered from other VA systems for use to test patches and upgrades prior to production deployment. There is no feasible means to collect data directly from the veteran. CPE does not have the ability to ensure that personally identifiable information is accurate, complete, and current. The source systems supplying VA data to CPE have procedures in place to verify/validate accuracy, currency, and completeness of the data. Source systems HealtheVet and Legacy VistA do collect information directly from the veteran.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

-

- Name – system testing- internal
- Social Security Number– veteran identification – system testing- internal
- Date of Birth– veteran identification – system testing- internal
- Mailing Address– system testing- internal
- Mother's Maiden Name– system testing- internal
- Phone Number(s) – system testing- internal
- Fax Number- system testing-internal
- Email Address– system testing- internal
- Financial Information – system testing- internal

- Emergency Contact Information – system testing- internal
- Health Insurance Beneficiary Numbers– system testing- internal
- Current Medications– system testing- internal
- Previous Medical Records– system testing- internal
- Race/Ethnicity– system testing- internal

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.

Please provide response here
The systems use data to provide a production-like environment for new and/or modified software to be tested. The data is not used for clinical purposes and therefore is not analyzed.

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.
Since CPE Preproduction VistA is not used for clinical purposes, new patient data is not created.

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 in transit and data at rest are encrypted.

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

CPE Preprodcution VistA does not collect new SSNs. Access controls are used to limit who can view and edit retained SSNs.

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

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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?

-
- The System of Record Notice (SORN) that applies to this system define the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for testing a multitude of pre-production systems/applications. This allows the VA to ensure patches, updates and coding changes are fully safe and functional prior to deployment in the active production environment. The types of controls that are in place for CPE PreProduction VistA are as follows: The minimum-security requirements for CPE's high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems

and the information processed, stored, and transmitted by those systems. The security related areas 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. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. Users are trained how to handle sensitive information by taking VA Privacy and Security Awareness Rules of Behavior training (mandatory for all personnel with access to sensitive information or access to VA network). After completing the course, users read and attest they understand the VA Rules of Behavior. Additionally, CPE users with access to PHI must also take VA HIPPA Focused training. All users must complete required training before gaining access to the CPE system. VA Privacy and Information Security Rules of Behavior training and HIPPA training are required to be taken on an annual basis. Role based access limits the scope and access the users have to information in CPE PreProduction VistA. Users with system administration privileges are mandated to accomplish additional System Administrator role-based training

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

- CPE Preproduction VistA access request form includes a list of rules of behavior that outline individual user's responsibilities in using the system. Additionally, users are required to have completed VA's annual information security training.

2.4c Does access require manager approval?

User access requests require Project Manager (PM) approval if an employee or COR approval if a contractor

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

- User logins are recorded in the VistA Kernel Sign-On Log file

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

- CPE Infrastructure staff follow defined procedures for granting system access

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Fax Number
- Phone Number(s)
- Email Address
- Emergency Contact Information
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity

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.*

CPE follows Records Control Schedule (RCS) 10-1 for retention of data which states: Electronic Input/Source Records.

Electronic records used to create, update, or modify records in an electronic recordkeeping system. Including:

- • Electronic files that duplicate information from a source electronic system for input into another electronic system
- • Electronic records received from another agency and used as input/ source records by the receiving agency (see exclusions)
- • Computer files or records containing uncalibrated and un-validated digital or analog data collected during observation or measurement activities or research and development programs and used as input for a digital master file or database
- • Metadata or reference data, such as format, range, or domain specifications which is transferred from a host computer or server
- • Another computer for input, updating, or transaction processing operations

Temporary; destroy immediately after data have been entered or otherwise incorporated into the master file or database and verified, but longer retention is authorized if required for business use. (DAA-GRS-2013-0001-0004, item 020)
EXCLUSION 1: Original electronic records maintained in the source system.
EXCLUSION 2: Electronic input records required for audit and legal purposes.
EXCLUSION 3: Electronic input records produced by another agency under the terms of an interagency agreement or records created by another agency in response to the specific information needs of the receiving agency.
[NOTE: not media neutral. Applies to electronic records only.]

3. **Output Records.**
Output records are records derived directly from the system master record. Examples include system generated reports (in hardcopy or electronic format), online displays or summary statistical information, or any combination of the above. By contrast, reports created using system information but not created directly from the system itself are not system output records, for example an annual report that agency staff prepares based on reviewing information in the system.
EXCLUSION 1: Query results or electronic reports created for a specific business need such as an established reporting requirement or a response to a formal request from a higher-level office of the agency or an entity external to the agency. Such records should be filed with an appropriate related series when applicable. If not applicable, these records must be scheduled.
EXCLUSION 2: Any hard copy records printed directly from the electronic systems that are not described below. Such records should be filed with an appropriate related series when applicable. If not applicable, these records must be scheduled.

6. Ad hoc reports. Reports derived from electronic records or system queries created on an ad hoc, or one-time, basis for reference purposes or that have no business use beyond immediate need. This item includes ad hoc reports created from or queries conducted across multiple linked databases or systems.

Temporary; destroy when business use ceases. (DAA-GRS-2013-0001-0005, item 030) Version Date:

EXCLUSION 1: Reports created to satisfy established reporting requirements (e.g. statistical reports produced quarterly in accordance with an agency directive or other regular reports to management officials).
EXCLUSION 2: Records containing substantive information, such as annotations, that is not included in the electronic records. (Reports that contain substantive information should be disposed of in accordance with a NARA-approved schedule that covers the series in which they are filed.)
b. Data outputs files. Data files or copies of electronic records created from databases or unstructured electronic records for the purpose of information sharing or reference, including:
• Data files consisting of summarized or aggregated information (See exclusions)
• Electronic files consisting of extracted information (See exclusions)
• Print files (electronic files extracted from a master file or database without changing it and used solely to produce hard-copy publications and/or printouts of tabulations, ledgers, registers, and statistical reports)
• Technical reformat files (electronic files consisting of copies of a master file or part of a master file used for information exchange) (See exclusions)
Temporary; destroy when business use ceases. (DAA-GRS-2013-0001-0006, item 031)
EXCLUSION 1: Data files that are created as disclosure-free files to allow public access to the data.
EXCLUSION 2: Data files consisting of summarized information from unscheduled electronic records or records scheduled as permanent but that no longer exist or can no longer be accessed.
EXCLUSION 3: Data extracts produced by an extraction process which changes the informational content of the source master file or database.
EXCLUSION 4: Technical reformat files created for transfer to NARA.
EXCLUSION 5: Data extracts containing Personally Identifiable Information (PII).
Such records require additional tracking and fall under GRS 4.2, item 15a (DAA-GRS-2013-0007-0012).

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

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

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

Yes

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

RCS 10-1 was approved January 2016 by NARA.

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from

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.

CPE minimizes the risk to privacy by limiting access to the CPE PreProduction VistA system on a role – based basis. Access is controlled as described in other sections of this document.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 by CPE 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 or breached.

Mitigation:

To mitigate the risk posed by information retention, CPE adheres to the NARA General Records Schedule 10-1. When the retention date is reached for a record, and the data has no further business use, the individual's information is carefully disposed of in accordance with VA policy.

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***
Master Person Index (MPI)	Source system supplying data for CPE test environment	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	HL7 electronic transmission
VHA Medical Facilities	Source system supplying data for CPE test environment	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	VHA Medical Facilities - SFTP
VA Office of Information and Technology (OI&T)	Source system supplying data for CPE test environment	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance	TCP/IP

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*
		Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	
Veterans Data Integration and Federation (VDIF)	Source system supplying data for CPE test environment	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Phone Number, fax Number, Email address, Emergency Contact Info, Health Insurance Beneficiary, Current Medication, Previous Medical Records, Race/Ethnicity, Financial Account Information.	Enterprise Cache Protocol (ECP)

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 privacy risk associated with transmitting PII within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation:

The principle of need-to-know is strictly adhered to by the CPE personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within it.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

			more than one)	
N/A				
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

Follow the format below:

Privacy Risk:

There is little or no risk for transfer of data externally. CPE does not share or received data outside of the VA boundary.

Mitigation:

There is no risk to mitigate for 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.

For VHA related Privacy Notification online can be found at: http://www.va.gov/health/ after getting to the website select VA Privacy Practices link (as shown below) on the lower right side of the web page. Additionally, the CPE Preproduction VistA system does not directly collect information from individuals. The SORN 121VA10 / 88 FR 22112 National Patient Databases-VA 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA.

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

Information is not directly collected from individuals. Rather, previously collected information from other VA systems is used.

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
.
Information is not directly collected from individuals. Rather, previously collected information from other VA systems is used.

The Department of Veterans Affairs does provide public notice that the CPE system does exist. This notice is provided in 2 ways:
1) The System of Record Notice (SORN) 121VA10 / 88 FR 22112 - National Patient Databases-VA (formerly 121VA19) The SORN can be found https://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-11487.pdf and 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

2) This Privacy Impact Assessment (PIA) also serves as notice of the CPE 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." http://www.oprm.va.gov/privacy/pia.aspx

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.

No information is directly collected from individuals by CPE. Therefore, there is no opportunity to decline to provide information input into CPE. Version Date: February 26, 2021 Page 25 of 38 A Veteran may have the opportunity and had been given notice of the right to decline to provide information to the source systems that collect the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to the CPE system and other downstream applications.

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.

No information is directly collected from individuals by CPE. Therefore, there is no opportunity to consent to particular uses of the information input into CPE. A Veteran may have the opportunity to consent to particular uses of the information given to the source systems that collect the information from the Veteran. By consenting to specific uses of information to the source system, the Veteran would also be consenting to specific use of the information to the CPE system and other downstream applications

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

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

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

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

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

<u>Privacy Risk:</u>

There is a risk that individuals are not provided sufficient notice of how their information will be used. Additionally, there is a risk that members of the public may not know that the CPE system exists within the Department of Veterans Affairs.

Mitigation:

As stated above in Section 6, VHA related Privacy Notification online can be found at: http://www.va.gov/health/ . The VA mitigates the system notification risk by providing the public with two forms of notice that the system exists, as discussed in detail above in question 6.1, including the Privacy Impact Assessment and the System of Record Notice. In addition to any applicable localized information use procedure, every system user must take VA Privacy and Security Awareness Rules of Behavior training on an annual basis which describes how information is to be used and the penalties for noncompliance. Users with access to Protected Health Information (PHI) must complete VA HIPAA Focused training annually.

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.***

As the CPE Pre-Production VistA systems is comprised of data records copied from production VistA instances, an individual seeking to access his/her own record would need to contact the FOIA point of contact for the source system. VA FOIA points of contact are available at https://department.va.gov/foia/

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).

Not applicable

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.

Not applicable

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.

As stated above in Section 7.1 the SORN has published the procedure for correcting inaccurate or erroneous information.

The following procedures are from VA Handbook 6300.4:

(1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b(3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.
(2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays)
(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will
corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."
(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70- 19, Notification to Other Person or Agency of Amendment to a Record, may be used.
(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which

the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record Under the Privacy Act, may be used for this purpose.
(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.
(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.
(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g)).
(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to
amend. The statement may contain information that the individual believes should be substituted.
(10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.

(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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 VA notifies individuals in two ways by publishing the SORN in the National Register and by publishing this PIA on the VA public website at: http://www.oprm.va.gov/privacy/pia.aspx

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.

Formal redress procedures are published in SORN 121VA10 / 88 FR 22112 (formerly 121VA19) National Patient Databases-VA. The SORN can be located online at: https://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-11487.pdf

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 erroneous information is placed into CPE via the feeds from VistA, HealtheVet and the VA WAN.

Mitigation:

The information in CPE PreProduction VistA is obtained via VistA, HealtheVet and the VA WAN. If there is erroneous or inaccurate information, it should be addressed in the VistA, HealtheVet and the VA WAN systems.
Any validation performed would merely be the Veteran personally reviewing the information before they provide it to the source systems feeding CPE. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.
HealtheVet allows Veterans to make changes to personal information in their profile via their online account logon.
In addition to any applicable localized information use procedure, every system user must take VA Privacy and Security Awareness Rules of Behavior training on an annual basis which describes how information is to be used and the penalties for noncompliance. Users with access to Protected Health Information (PHI) must complete VA HIPAA Focused training annually

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.

CPE components rely on the underlying enterprise infrastructure to manage information system accounts. There are automatic notifications regarding account changes.

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?

Users from agencies other than the VA do not access CPE systems.
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 users requesting access must complete a CPE Access Request form. The form must clearly indicate the specific access requested and the user needing the access. The form must be signed by the requestor and endorsed by the requestor's supervisor in the case of an employee or by the requestor's Contracting Officer Representative in the case of a contractor.

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.

VA contract employee access is verified through the Contracting Officer's Representative and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.
Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.
Contracts include a Security and Privacy Requirements section that is binding on the contractor. In this section the position sensitivity and level of background investigation for each contract task are identified. Any contractor working on a specific task must satisfy the identified Background Investigation level.
Contractors have access to the system and the PII/PHI contained in it. Contractors access the system for the purposes of software application development and testing. This typically involves the installation of new or modified application source code, the execution of a test plan in order to observe the performance of the new or modified code and the capturing of test plan results for analysis.

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.

Personnel that will be accessing VA sensitive information or VA information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or

VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

Yes, ATO renewed on February 27, 2023 for 180 days

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 5/23/2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 11/24/2023
5. *The Authorization Termination Date:* 11/24/2023
6. *The Risk Review Completion Date:* 10/4/2023
7. *The FIPS 199 classification of the system 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.***

ATO renewed on August 11, 2023 for 90 days

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 does not currently utilize cloud technology.

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.*

Not applicable

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.

Not applicable

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.

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).

The system does not currently utilize RPA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2023.09.14 08:22:11 -05'00'

Privacy Officer, Lynn Olkowski

Craig J. Heitz 564885

Digitally signed by Craig J. Heitz 564885
Date: 2023.09.12 08:42:22 -05'00'

Information System Security Officer, Craig Heitz

ANTHONY LENGVINIS

Digitally signed by ANTHONY LENGVINIS
Date: 2023.09.11 15:58:11 -04'00'

Information System Owner, Tony Lengvinis

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).

SORN 121VA10 / 88 FR 22112 (formerly 121VA19) National Patient Databases-VA. The SORN can be located online at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices