Privacy Impact Assessment for the VA IT System called:

Veteran's Informatics Computing Infrastructure (VINCI)

Data and Analytics

Date PIA submitted for review:

5/8/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	kimberly.murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Patricia Alleyne	Patricia.Alleyne@va.gov	512-809-7532
Information System Owner	Jeremy Gebhard	Jeremy.Gebhard@va.gov	360-566-7302

Abstract

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

Veteran's Informatics Computing Infrastructure (VINCI) is an analytical platform providing secure access to VA data and software in a high-performance computing environment. The researchers using the VINCI data are prevented by a firewall from extracting, downloading, changing, or deleting any data from VINCI but can use that data for their research projects. There is no ability for users to transfer data into or out of VIN, except by VIN system administrators. VIN is primarily used by VHA Office of Research and Development (ORD). It has access to all data in the Corporate Data Warehouse (CDW), which hosts a substantial amount of current as well as historical clinical data. VINCI is primarily used by VHA Office of Research and Development (ORD).

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.

Veterans Informatics and Computing Infrastructure , Data and Analytics

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

Veteran's Informatics Computing Infrastructure (VINCI) is a joint partnership between VA Office of Information & Technology (OI&T) and VHA Office of Research and Development (ORD). The OI&T and Product Engineering (PE) owns Data and Analytics which is integrating data from multiple VA data sources to populate the national the Corporate Data Warehouses (CDW) which VINCI is a shadow.

Because the activities of the VINCI and CDW are highly complementary, this partnership provides significant efficiencies in VINCI work. VINCI provides the greater VA research community information technology and services that minimize the risk of veterans' data loss and improves appropriate access to and use of Veterans' data for research purposes.

C. Indicate the ownership or control of the IT system or project.
Department of Veterans Affairs

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.
VINCI warehouses information on all veterans in the VA health system. There is currently health data for approximately 15 million veterans in VINCI.

E. A general description of the information in the IT system and the purpose for collecting this information.
VINCI doesn't collect information but instead uses information already collected by other VA systems. The data is used by researchers.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
Corporate Data Warehouse (CDW) and VINCI share data veterans' health data.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
All VINCI systems and data are hosted at Austin Information Technology Center

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.
VHA Corporate Data Warehouses-VA'' (172VA10/ 86 FR 72688) a 2021-27720.pdf (goVINCIfo.gov) and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10/85 FR 84114) 2020-28340.pdf (goVINCIfo.gov)e here

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
No. Currently no cloud storage or use.

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)

PII Mapping of Components (Servers/Database)

Veteran's Informatics Computing Infrastructure **(VINCI)** consists of **six** 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 Veteran's Informatics Computing Infrastructure (**VINCI)** 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
VA Corporate Data Warehouse	No	Yes	Name, SSN, DOB, mother's maiden name, mailing address and zip code, email address, emergency contact info, current medications, previous medical records and race/ethnicity and gender	VINCI doesn't collect PII Data. The Data are updates from existing CDW databases	Databases\ Storage Arrays use FIPS 140-2 Encryption. Access controlled via Active Directory permissions

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?

Most of the data in VINCI system comes from the Corporate Data Warehouse (CDW). There is also Medical Statistical Analysis System (MedSAS), CDC. NIH (via source CDW system), Health Economics Resource Center (HERC) data, DoD and VA Research study from individual researcher data. VINCI also receives derived data from National Institutes of Health (NIH), Centers for Disease Control and Prevention (CDC), Medicare, and Medicaid via CDW.

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.

All VINCI data is from other VA entities through Corporate Data Warehouse and is not a data source but is a data warehouse

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

Most of the data in VINCI system comes from the Corporate Data Warehouse (CDW). There is also Medical Statistical Analysis System (MedSAS), CDC. NIH (via source CDW system), Health Economics Resource Center (HERC) data, DoD and VA Research study from individual researcher data

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?

VINCI is a shadow to Corporate Data Warehouse collects information from the VISN Data Marts, Regional Data Warehouses into the system. This data is transferred from CDW via the VA Local Area Network secure behind a firewall. Data is received via secure electronic transmission. CDW receives the data from other sources such as the VISTA systems and does not collect data itself

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.

N/A

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.

Accuracy is based on quality of data from CDW. That data comes from other sources such as the VISTA Systems. Information is checked for accuracy by source systems of CDW prior to transfer to VINCI. A comparison is done by matching CDW fields to the VistA source data.

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.

N/A

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

As stated in System of Record Notice (SORN) 121VA19 - National Patient Databases-VA, Title 38, United States Code, Section 501 is the authority for maintenance and operation of this system. Additionally, VA Research data is collected under the authority of Title 38 United States Code (U.S.C), 7303

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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: There is a risk that data contained in the VINCI may be shared with unauthorized individuals or that authorized individuals may share it with other unauthorized individuals.

Mitigation: All users requesting access to the VINCI systems including DaVINCI are authorized through the Data Access Request Tracker (DART) application by National Data Systems (NDS) personnel to mitigate the risk of unauthorized users. The DART is how users get access to VINCI. Department of Veterans Affairs is careful to only collect the information necessary to complete the mission of the Office of Research and Development (ORD). Once an incident is reported, the VA makes all efforts to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information. There is only one path to get data into or out of VINCI and every transfer in either direction is audited and copied in its entirety. VINCI also copies and checks each file to confirm that any data leaving has been properly authorized by NDS.

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**: Used to identify the veteran.
- **Social Security Number**: Used to identify Veterans and are inherent to the data used for research within VINCI.

- **Date of Birth**: Used to verify the identity of the veteran– Used for statistical reporting
- **Mailing Address**: Used to verify the identity of the veteran- communication
- **Mother's Maiden Name**: Used to verify the identity of the veteran
- **Phone Number(s)**: Communication with veteran
- **Personal Email**; Communication with veteran
- **Emergency Contact Information** (Name, Phone Number, etc. of a different individual): Used to communicate with veteran's next of kin
- **Current Medications**: Used to record current health and medical conditions of the veterans such as: Hepatitis C registry, Human Immunodeficiency Virus (HIV) registry, problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, statistical reporting and operations.
- **Previous Medical Records**: Used to record the history of health and medical conditions of the veterans such as: Hepatitis C registry, Human Immunodeficiency Virus (HIV) registry, problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, statistical reporting and operations.
- **Race/Ethnicity**: Used for statistical reporting and research
- **Gender**- Used to identify the veteran

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.

VINCI contains commercial and custom software that primarily targets research needs. VINCI uses a variety of software including SAS, R, Hadoop, Stata, Matlab, SPSS, Microsoft SQL (MSQL), and a host of other software. Users within VINCI have access to a substantial amount of current as well as historical clinical data used primarily for VA research and protected behind the VINCI Firewall.

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

The system does not create new data or make available any new data.

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?

The VINCI data is encrypted at rest and in transit by VA network encryption standards.

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

Implemented jointly between OIT and VHA, end users who have access to SSN must request a specific authorization. General end users do have access to patient or employee SSN.

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

The VINCI data is encrypted at rest and in transit by VA network encryption standards.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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 minimum-security requirements for VINCI's medium 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. The security control implementation within the VINCI system is recorded within the System Security Plan (SSP) and is placed in the official system records repository system called Risk Vision. The VINCI application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 and VA directives or handbooks. VA Records Management Policy (VA Handbook 6300.1) and the VA Rules of Behavior are in place to mitigate some of the risk that information is not handled properly. All VA annual privacy and security awareness training is recorded in the Talent Management System (TMS), a VA training system. The rules of behavior (VA handbook 6500 appendix D) govern how veterans' information is used, stored, and protected.

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

Yes it is part of the NDS SOP and intake process

2.4c Does access require manager approval?

Manager approval is required by NDS for VINCI data access.

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

Access is managed and tracked by two applications, BaseCamp and DART

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

All VA employees, the Information Systems Owner and Information system Security Officer.

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
- Phone Number(s)
- Emergency Contact Information

- Current Medications
- Previous Medical Records
- Race/Ethnicity
- VA Benefits Information

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.*

VINCI data is retained until the VINCI Governance Board approves a policy for records disposition. Records Schedule Number DAA-0015-2015-0004 was approved by the National Archives and Records Administration (NARA) and published on 7/13/2015. The records schedule has various retention lengths for data types within VINCI. Once the VINCI Governance Board approves, records will be retained in accordance with the new records schedule. The records schedule can be found at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2015-0004_sf115.pdf An example of non-research data: General Program Records relating to ORO's general administration and operation of VA's intramural research programs and the conduct of research are listed for cut off at the end of the fiscal year after final action. The retention period is to destroy no sooner than 3 years but no later than 6 years after cutoff.

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

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

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

Documentation is available on VINCI Central (vaww.VINCI.med.va.gov) and from VINCI document master. Records Schedule Number DAA-0015-2015-0004 was approved by the National Archives and Records Administration (NARA) and published on 7/13/2015.The records schedule can be found at http://www.archives.gov/recordsmgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2015-0004_sf115.pdf and https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2015-0004_sf115.pdf

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

Transitory records. Records required only for a short time (generally less than 180 days) and that are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision. Destroy when no longer needed for business use or according to the agency predetermined time period or business rule. DAA-GRS-2017-0003-0001.

Intermediary records. Records of an intermediary nature, meaning that they are created or used in the creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of document or file, or when decision-making. Destroy upon verification of successful creation of the final document or file or when no longer needed for business use, whichever is later. DAA-GRS-2017-0003-0002

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. Austin Information Technology Center (AITC) has an exception memorandum, dated 13 Apr 2015, allowing the center to locally destroy media. The memorandum lists specific methods of sanitization which are approved methods in accordance with VA 6500. 1..
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 printers.
AITC has a local shred contract (VA200R-1307) covering the destruction of printed data.

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.

a) VINCI tests new or modified IT systems for VINCI operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VINCI policy. In addition, VINCI may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VINCI policy PII and PHI may be used for that training purpose. However, VINCI must minimize the use of PII and PHI in training presentations or materials per VA policy.VA Research investigators may use PII for VA Institutional Review Board (IRB)-approved research, and there is no effort to minimize the use of PII for research.
b) Controls for protecting PII used for testing, training and research for IT system development and deployment are often security controls if the PII is electronic. When paper PII, reasonable safeguards for protecting the PII are to be employed.
Reference: - VA IS Reference Guide SA11- no live data in test.pdf DM-03.1 VA Handbook 6507.1.pdf

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VINCI 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, VINCI adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the data is carefully

disposed of by the approved method as described in Records Schedule in accordance with VA 6500.1 HB media and destruction policies.
Records Schedule Number DAA-0015-2015-0004 was approved by the National Archives and Records Administration (NARA) and published on 7/13/2015.

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***
VHA Office for Analysis and Business Intelligence	Research requests for business analysis supporting veterans	• Name • Social Security Number • Date of Birth • Mothers Maiden	Secure electronic data transfer via online connection to VINCI

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*
	through VA statistical analysis, reporting and leadership decisions	Name • Mailing Address • Phone Number(s) • Emergency Contact Information • Current Medications • Previous Medical Records • Race/Ethnicity • VA Benefits Information	database. File Transfer over Sockets Layer (SSL) /Transport Layer Security (TLS) Remote Desktop Communication (RDP over SSL/TLS)
VHA Office of Research Development	Research request supporting VA research projects helping veterans by supporting information in medical and other research. Research studies supply data to VINCI and use data within VINCI	• Name • Social Security Number • Date of Birth • Mothers Maiden Name • Mailing Address • Phone Number(s) • Emergency Contact Information • Current Medications • Previous Medical Records • Race/Ethnicity • VA Benefits Information	Secure electronic data transfer via online connection to VINCI database. File Transfer over Sockets Layer (SSL) /Transport Layer Security (TLS) Remote Desktop Communication (RDP over SSL/TLS)
Veterans Health Administration	Research requests for business analysis supporting veterans through VA statistical analysis, reporting and leadership decisions	Name, SSN, DOB, mother's maiden name, mailing address and zip code, email address, emergency contact info, current medications, previous medical records and race/ethnicity	File Transfer over Sockets Layer (SSL) /Transport Layer Security (TLS)

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: There is a risk that data contained in the VINCI may be shared with unauthorized individuals or that authorized individuals may share it with other unauthorized individuals. Examples of this risk would be an unauthorized person breached the system or a VA sponsored user shares data outside of the VA boundary without express written permission.

Mitigation: All access to VINCI data is authorized through the Data Access Request Tracker (DART) system and is controlled by National Data Systems (NDS) team. All research users are screened by an approval process prior to gaining access to VINCI in order to mitigate unauthorized users. The process includes approvals from a Research Study's Principal Investigator (PI). Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA Talent Management System (TMS). Business users are screened by the Corporate Data Warehouse (CDW) and other business unit management team staff before being submitted for an access request to NDS.
Study data will be kept in accordance with the Department of Veterans Affairs record control schedule 10-1 (RCS 10-1). Upon completion of the research project, the PI in conjunction with the VA Information Security Officer (ISO), and in accordance with VA 6500 HB and all relevant VA policy, will ensure that, study data containing sensitive, confidential information will be returned to the VA, sanitized and removed from all servers, desktops, removable storage devices, etc. When any study personnel are no longer a part of the research team, the PI will remove that person's access to all study data and notify the VA Information Security Officer of such action. VINCI personnel will be responsible for maintaining VINCI servers where study data will be kept. It will be VINCI personnel who will move, backup and remove study data from VINCI servers and who will control access to data stored on VINCI servers. The PI will request termination of data access rights for study personnel who are no longer part of the study team.
The workspace request process is described on the following website:
http://vaww.vhadataportal.med.va.gov/DataAccess/VINCIWorkspaceRequestProcess.aspx

Section 5. External Sharing/Receiving and Disclosure

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

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

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Department of Defense DHA-MID Enclave	The purpose of information being shared is to support clinical operations and research projects within the VA and DoD/DHA.	DoD/DHA EMR and claims data, DoD/DHA enrollment and eligibility information, DoD/DHA OMOP data.	MOU/ISA	Site to Site (S2S), IPSEC Tunnel, Secure FTP

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 limited risk for external sharing of data contained in the VINCI system. Access to VINCI data is only through the VA Local Area Network and not directly from external users.

Mitigation: Currently, there is only one authorized external connection to the VINCI system (Department of Defense). All data access is authorized by NDS prior to a user being granted access. All users must be VA sponsored and must obtain a VA user account to access the VINCI system.
The data, applications and virtual computing used by the VA business users reside behind the GSS in the Austin Information Technology Center. User will use Microsoft Remote Desktop Connection (RDP), or SQL Server Management Studio (SSMS) to access virtual computing sessions from their local workstation. Microsoft RDP and SSMS software uses a VA-approved secure communications protocol between the local workstation and the VINCI SQL servers and requires valid VA user account with authorized access to that system/database. There is no World Wide Web access from servers all sites are internal to the VA only.
All users that have access to VINCI must read and acknowledge the rules of behavior certifying (with digital signature) they understand the policies of working with VA data (sensitive or otherwise) and will abide by all restrictions set forth in VA policy. This training and awareness are completed in TMS and reaffirmed annually.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

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

The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy.

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

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

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices 172VA10P2, 121VA10A7, and 79VA10P2. When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

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

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

The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices 172VA10P2, 121VA10A7, and 79VA10P2. When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.VHA Directive 1605.01 Privacy and Release Information', lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA.

The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)). The VINCI system receives its data from CDW whose gets the bulk of source data from the VISTA system; therefore, notice of the right of refusal would be addressed by source system. Notice and Right to Decline are provided by research protocols supplying information to the VINCI system. A Privacy Act Notice is provided to active participants of VA research studies. If a participant in a research study declines to provide information the participant may not be eligible to continue to participate in the research study. In accordance with VHA Handbook 1200.05, a written HIPAA authorization signed by the individual to whom the information or record pertains is required when VA health care facilities need to utilize individually-identifiable health information for a purpose other than treatment, payment, or health care operations (e.g., research).

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN). When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that members of the public may not know that the VINCI system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk of not providing notice to the public as discussed in detail in question 6.1 above, the PIA and SORN 172VA10P2, 121VA10P2, 79VA19 are published to notify and inform the public that information collected by the VA is stored in the VINCI system. Active participants in research studies are given notice and informed consent documents prior to their information being collected for the study.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to obtain more information about access, redress and record correction of VINCI system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 121VA19 - National Patient Databases-VA. This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf.
The VA Privacy Service monitors and documents any anomalies or problems to improve the Privacy controls. This control is the responsibility of the VA. The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN). When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII. Individuals wishing to obtain more information about access, redress and record correction of CDW system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 121VA10A7 - National Patient Databases-VA. This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf

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

N/A

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

N/A

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

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

Individuals wishing to obtain more information about access, redress and record correction of VINCI system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 121VA19 - National Patient Databases-VA. This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf

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 Privacy Service monitors and documents any anomalies or problems to improve the Privacy controls. This control is the responsibility of the VA. Individuals wishing to obtain more information about access, redress and record correction of CDW system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 10A7 National Patient Databases-VA. This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf.

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.

Not applicable, formal redress is provided as stated above in section 7.3.

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: This section is not applicable to VINCI. Individuals do not access their records through this system so the risk is low.

Mitigation: This section is not applicable to VINCI. Individuals do not access their records through this system so the risk is low.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. All data access is authorized through the data access request process used by National Data Systems (NDS) prior to a user being granted access. VINCI relies on Enterprise Operations who each month issues a list of 90 day inactive and expiring user accounts. System administrators then take the appropriate action. OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed using Talent Management System (TMS).

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?

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are 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 TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate Version Date: January 2, 2019 Page 21 of 19background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training (TMS#10203) is required initially and annually thereafter

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.

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are 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 TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate Version Date: January 2, 2019, Page 21 of 19 background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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

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

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training (TMS#10203) is required initially and annually thereafter.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 2 February 2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 31 Mar 2023
5. *The Authorization Termination Date:* 14 Jul 2023
6. *The Risk Review Completion Date:* 27 Mar 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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)*

VINCI does not currently use 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.*

VINCI does not currently use cloud technology

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.

VINCI does not currently use cloud technology

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.

VINCI does not currently use cloud technology

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).

VINCI does not currently use Robotics Process Automation (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**

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.06.01 16:23:19 -04'00'

Privacy Officer, Kimberly Murphy

PATRICIA ALLEYNE

Digitally signed by PATRICIA ALLEYNE
Date: 2023.05.24 10:27:58 -05'00'

Information System Security Officer, Patricia Alleyne

JEREMY GEBHARD

Digitally signed by JEREMY GEBHARD
Date: 2023.05.24 08:12:31 -07'00'

Information System Owner, Jeremy Gebhard

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).

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