Privacy Impact Assessment for the VA IT System called:

Analytics and Business Intelligence LAN (KSS)

Office of Informatics and Analysis

Veterans Health Administration (VHA)

Date PIA submitted for review:

11/18/2022

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)	James Alden	James.Alden@va.gov	781-687-4779
Information System Owner	Scot Dingman	Scot.Dingman@va.gov	512- 326-6645

Abstract

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

The Analytics and Business Intelligence (ABI) LAN provides timely and reliable analytic and business intelligence data and products to support and improve clinical and operational programs at all levels of the VHA health care delivery system. ABI LAN's sophisticated analytic and business intelligence solutions facilitate evidence-based decisions for Veterans and their families, patient populations, clinicians, and those managing health care delivery 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.

The Analytics and Business Intelligence (ABI) LAN, also known as the VHA Support Services Center (VSSC) and owned by the Veterans Health Administration (VHA) Office of Informatics and Analytics, is a system comprised of servers, printers, Storage Area Networks (SAN), tape drives and switches that support the display of management reports to the Department of Veterans Affairs (VA).

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

The vision of the ABI LAN is to create tools and knowledge that will foster the operation of high value, high quality, safe, and patient-centered healthcare systems for Veterans. The system includes a wide variety of tools and applications including but not limited to SQL databases, SAS data processing systems, web presentations, and report utilities for analyzing data sets. The data provided by these reports assists management in VA medical centers and in Headquarters to better manage scarce Veteran resources.

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

Where applicable, ABI LAN reports have restricted access to Protected Health Information (PHI), or Personally Identifiable Information (PII). These special reports require that the user complete VA Form VA Form 9957 which is signed by the user's Supervisor to approve access and submitted via their local Customer User Provisioning (CUPS) point of contact who will complete the necessary steps to obtain the access.

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 data provided by these reports assists management in VA medical centers and in Headquarters to better manage scarce Veteran resources. ABI LAN reporting services are provided through the ABI LAN Portal in the form of subscription ready reports; automatic e-mail delivery as soon as data is updated; Statistical Analysis System (SAS) scanned reports; easy to use standard output; Pyramid Analytics reports; retrieval of multiple years of data or multiple facilities data quickly; design of user's own report

format so it will automatically update when underlying data is updated; exploratory Analysis – add or remove variables from query quickly; SQL Server Analysis Server cube data; executive views of data; and detailed analysis capabilities, and many other features.

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

The ABI LAN is hosted at the Austin Information Technology Center (AITC), a data center under Enterprise Operations (EO). The number of individuals whose information is stored on ABI is over 9,000,000 comprising of Veterans, dependents, VA contractors, volunteers, clinical trainees, and VA employees. The purpose of information collecting in the ABI LAN is to create tools and knowledge that will foster the operation of high value, high quality, safe, and patient-centered healthcare systems for Veterans.

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

ABI LAN data is collected electronically from the Veterans Health Information Systems and Technology Architecture (VistA), other VA internal systems, and the VA Data Warehouse. ABI LAN does not collect PII/PHI directly from individuals.

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.

Where Appropriate (ABI) LAN uses Microsoft Windows Authentication including Multi-Factor with PIV Cards and USB E-Tokens, SSL Encryption (FIPS Compliant TLS 1.2 Encryption), Kerberos Encryption/Authentication, Microsoft Windows NTFS Security for File Shares, OAUTH, & Microsoft SQL Server Authentication.

3. Legal Authority and SORN

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

ABI LAN's legal authority can be found in Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Sections 501(a), 1710, 1729 and Section 7304, Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55. ABI LAN is covered under System of Records Notice (SORN) 79VA10 and 121VA10A7.

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 SORN amendment is required. The SORN that governs cloud usage has been approved by the KSS - Business Analytics and Business Intelligence LAN PTA, approved in October 2022. All VA email is stored in the private Azure cloud called MAG (Microsoft Azure for Govt) with Microsoft. Teams Data is stored in the cloud. Any Office 365 product might be stored in the private cloud. The Analytics and Business Intelligence (ABI) LAN have Power BI data that is being stored in the private MAG cloud. These are enterprise VA contracts/agreements. Some (ABI) LAN data is pushed to Palantir Foundry (https://va.palantirgov.com) and there is an existing Memorandum of understanding (MOU) for that.

There is also a Wait Time data that is put in the public Microsoft Azure cloud for some contractors, and they produce a report for public consumption so folks know how long a wait would be at a facility, but that is also an Enterprise Agreement with Microsoft.

D. System Changes

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

No business practice changes will be required.

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

Completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series

(https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>> - N/A
*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical) – N/A

PII Mapping of Components (Servers/Database)

Analytics Business Intelligence LAN consists of 56 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 Analytics Business Intelligence LAN 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
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; Secure Socket Layer (SSL) encryption; and National Social Security Database (NSSD).
Development SQL server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL / Cube / Database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL / Cube / Databases server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube Server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL / Cube / Database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Development External connection SQL/Cube / Oracle server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL / Cube / Database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production SQL / Cube / Database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Power BI server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Power BI server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Power BI server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL / Cube / Database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production Application server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Application server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SQL / Cube test server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production SQL Server Reporting Servers (SSRS) server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Staff File Shares server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development GeoMapping / ArcGIS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SharePoint to load-balance server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SQL SSRS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production SharePoint frontend server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SharePoint database server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development SharePoint and temporary SSR redirects server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SharePoint Team Foundation server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SAS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production SAS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SharePoint Office Online server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 1	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 2	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 3	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Virtual Machine (VM) Host 4	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 5	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 6	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Virtual Machine (VM) Host 7	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production Geo Mapping/ ArcGIS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production SSRS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Development Web server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SSRS farm	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production ColdFusion and Help Desk server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production Web server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

Production Web server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production SSRS server	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD
Production Web server main VSSC site	Yes	Yes	All	National reporting	In order to gain access an electronic VA Form 9957 must be completed (https://epas.r02.med.va.gov/). In addition, there is windows, Kerberos, and SQL server authentication; Window file sharing security; McAfee anti-virus and intrusion detection; windows firewall; web-based firewall; SSL encryption; and NSSD

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?

Data available through the ABI LAN is collected electronically from VistA via SAS files from VistA systems that contain PII/PHI. ABI LAN does not collect PII/PHI directly from individuals.

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.

For the Homeless program, ABI LAN also receives electronic files from the VA's Homeless Management Information Systems (HMIS) hosted at the AITC. All data transmitted to ABI LAN is for healthcare operations, management, oversight, performance, and evaluation.

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

N/A

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?

ABI LAN data is collected electronically from VistA via SAS files from VistA systems that contain PII/PHI. VistA is the source of data for many VHA datasets to include: VHA Medical SAS datasets, VHA Decision Support System (DSS) National Data extracts, Pharmacy Benefits Management (PBM) data, and Veterans Integrated Service Networks (VISN) data warehouses, Corporate Data Warehouse (CDW). ABI LAN does not collect PII/PHI directly from individuals. For the Homeless program, ABI LAN also receives electronic files from the VA's Homeless Management Information Systems (HMIS) hosted at the AITC.

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.

The ABI LAN system assumes that the original source data was checked for accuracy when it was first entered into the source systems. Data can be checked for completeness by system audits, manual verifications and annual questionnaires through automated Veteran letters.

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

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Sections 501(a), 1710, 1729 and Section 7304, Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the ABI LAN. Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies. Public Law 99–272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986.

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:

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The ABI LAN collects and stores large amount of PHI/PII. Therefore, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, or misused, serious personal/professional or financial harm may result for the individuals affected. Additionally, the compromise of this information would constitute a breach of confidence with the Veterans served by the VA.

Mitigation: ABI LAN components rely on the underlying enterprise infrastructure for file system protection as outlined in the Enterprise Infrastructure Support (EIS) SSPs. Application data is protected by user access permissions. Data confidentiality and integrity is also ensured via administrative, technical and physical controls. Physical access to Enterprise Operations (EO) servers is restricted to authorized personnel in a data center at a facility with 24-hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers.
Employing user logon access controls, strict VA and Office of Inspector General (OIG) policies with training, and a physically secure facility are all controls that aid in keeping the data confidential. VA 6500 implementation of this control states that database management systems used in VA will be encrypted using FIPS 140-2 (or its successor) validated encryption. The encryption of database management systems is not currently implemented within EO. ABI LAN users will submit a completed access request application using a VA Form 9957. To ensure accountability, all user accounts on VA information systems must be individualized. Use of individual passwords is mandated. User Identification (user ID) and associated passwords are personal to the individual owner and must be chosen and protected with care. Only the user to whom the passwords are assigned will use the passwords. All passwords are considered sensitive information and must be treated as such. They may not be shared with anyone. Users are accountable for actions performed with their user ID and will be held liable for actions determined to be intentionally malicious, grossly negligent, or illegal. A user may not log on to any Enterprise Operations (EO) system or network unless they are properly registered in and authorized to use that system or network.

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 person
SSN: Used to verify the person's identity
Date of Birth: Used to verify the person's identity
Mother's Maiden Name: Used to identify Veteran patient records
Personal Mailing Address: Used to identify Veteran patient records
Personal Phone Number: Used to identify Veteran patient records
Personal Email Address: Used to identify Veteran patient records
Emergency Contact Information: Used to identify Veteran patient records
Health Insurance Beneficiary Numbers: Used to identify Veteran patient records
Current Medications: Used to record current health and medical conditions of Veteran such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Previous Medical Records: Used to record the history of health and medical conditions of the Veteran such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Race/Ethnicity: Used to identify Veteran patient records

The records and information available through ABI LAN's portal may be used for statistical analysis to produce various management, workload tracking, and follow-up reports; to track and evaluate the ordering and delivery of equipment, services, and patient care; for the planning, distribution, and utilization of resources; to monitor the performance of Veterans Integrated Service Networks (VISNs), and to allocate clinical and administrative support to patient medical care. The data may also be used for VA's extensive research programs in accordance with VA policy.

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.

The vision of the ABI LAN is to create tools and knowledge that will foster the operation of high value, high quality, safe, and patient-centered healthcare systems for Veterans. The system includes a wide variety of tools and applications including but not limited to SQL databases, SAS data processing systems, web presentation, and report utilities (e.g., Pyramid Analytics, Microsoft's SQL Server Reporting Services) for analyzing data sets. The data provided by these reports assists management in VA medical centers and in Headquarters to better manage scarce Veteran resources.

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.

N/A

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?

SSL Encryption (FIPS Compliant TLS 1.2 Encryption), Kerberos Encryption/Authentication.

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

KSS (ABI) LAN uses Microsoft Windows Authentication including Multi-Factor with PIV Cards and USB E-Tokens, Microsoft Windows NTFS Security for File Shares, OAUTH, & Microsoft SQL Server Authentication.

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

Where Appropriate (ABI) LAN uses Microsoft Windows Authentication including Multi-Factor with PIV Cards and USB E-Tokens, SSL Encryption (FIPS Compliant TLS 1.2 Encryption), Kerberos Encryption/Authentication, Microsoft Windows NTFS Security for File Shares, OAUTH, & Microsoft SQL Server Authentication.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to KSS PII is determined by the Information System Owner (ISO) and is issued on a Need-to-Know basis.

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

VA The Information System Owner (ISO) in conjunction with the Information System Security Officer (ISSO) and Privacy Officer (PO) monitor and audit privacy controls continuously and ensure self-assessments or third-party audits result in reports on compliance gaps identified in programs, projects, and information systems.

2.4c Does access require manager approval?

Access to KSS PII is determined by the Information System Owner (ISO) and is issued on a Need-to-Know basis.

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

The KSS Information System Owner ensures PII is being monitored and delegates the tracking/recording of access to the designated system administrator/responsible designee. The VA Chief Privacy Officer (CPO) defines the frequency for monitoring privacy controls and internal privacy policy to ensure effective implementation.

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

The Information System Owner (ISO) in conjunction with the Information System Security Officer (ISSO) 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*

ABI LAN data is collected electronically from VistA. In addition to the items listed in section 1.1 (name, SSN, date of birth, mother's maiden name, personal mailing address, personal phone numbers, personal email address, emergency contact, health insurance, medications, medical records, and race/ethnicity), PII/PHI data collected could also include medical benefit and eligibility information, information related to medical examination or treatment, diagnoses, medical facilities providing examination or treatment, information related to military service and status, Veteran homeless program, patient aggregate workload data such as admissions, discharges, and outpatient visits, resource utilization such as laboratory tests, x-rays, etc. Data collected from the interconnection with the United States Air Force includes enrollee and patient demographics (excluding patient names and real social security numbers), purchased care data, including type of

healthcare resource purchased, volume of resource purchased, dollars spent and vendor name, workload for inpatient and outpatients including diagnoses, discharges and encounters, and physician staffing numbers by provider specialty.

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.*

Retention period is seven (7) years for each electronic data transaction. Records Control Schedule (RCS) 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdfRecords Control Schedule (RCS) VB-1, Part II Revised for VBA: https://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.docNational Archives and Record Administration: www.nara.gov.

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?

RCS 10-1 (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) and RCS VB are approved by NARA (https://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc).

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

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.

3.4 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 including 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 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.

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.

N/A - No KSS PII/PHI data is used for research, testing, or training.

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 available through ABI LAN 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, the ABI LAN adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Information Systems and Technology Architecture (VistA/CPRS/AITC Mainframe)	Delivering services, information, and analysis in areas such as business operations, capital and planning, clinical care, customer service, quality and performance, resource management, and special focus programs.	Name, Social Security Number, Date of Birth, Mother's maiden name, Address, Phone Number, Fax Number, Email, Emergency contact information, health insurance beneficiary numbers, current medications, previous medical records, race/ethnicity.	Retrieval of data using SAS Connections to the AITC Mainframe.
VHA Decision Support System (DSS)	Delivering services, information, and analysis in areas such as business operations, capital and planning, clinical care, customer service, quality and performance, resource management, and special focus programs.	Name, Social Security Number, Date of Birth, Mother's maiden name, Address, Phone Number, Fax Number, Email, Emergency contact information, health insurance beneficiary numbers, current medications, previous medical records, race/ethnicity.	Transferred using SQL Server to SQL Server connections.
Pharmacy Benefits Management (PMB)	Delivering services, information, and analysis in areas such as business	Name, Social Security Number, Date of Birth, Mother's maiden name, Address, Phone	Sample: IPSEC Tunnel using SSL encryption.

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*
	operations, capital and planning, clinical care, customer service, quality and performance, resource management, and special focus programs.	Number, Fax Number, Email, Emergency contact information, health insurance beneficiary numbers, current medications, previous medical records, race/ethnicity. .	
Corporate Data Warehouse (CDW)	Delivering services, information, and analysis in areas such as business operations, capital and planning, clinical care, customer service, quality and performance, resource	Name, Social Security Number, Date of Birth, Mother's maiden name, Address, Phone Number, Fax Number, Email, Emergency contact information, health insurance beneficiary numbers, current medications, previous medical records, race/ethnicity.	Transferred using SQL Server to SQL Server connections.

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 ABI LAN provides access to large amount of Veteran data which is necessary by VA programs for the purposes of healthcare operations, management, oversight, and performance evaluation. The compromise of this information would constitute a breach of confidence with the Veterans served by VA.

Mitigation: The source data used in ABI LAN already exists in the other systems, and the electronic transfers of information are secure. All access is done through secure internal VA networks. Only selected users have access to PHI data. All users sign adherence to VA's strict privacy and security controls and must be current on VA Privacy and Information Security Awareness Rules of Behavior training. A properly executed VA Form 9957 is required for access to ABI LAN as described in section 1.7.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	with the specified program office or IT system		***use, etc. that permit external sharing (can be more than one)***	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: N/A

Mitigation: N/A

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 Department of Veterans Affairs provides public notice that the information is being collected. This notice is provided in two ways:

1. The System of Record Notices (SORNs): 79VA10 – National Patient Databases – VA, and 121VA10A7 – National Patient Databases – VA. Links to these SORNs are listed in section 2.3 above.
   https://www.oprm.va.gov/docs/SORN/Current_SORN_List_10_21_2022.pdf

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

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

ABI LAN System of Record Notice (SORN) and Privacy Impact Assessment (PIA) are available for review online, as discussed in Item 6.1a. No information is collected directly from individuals and that the source systems have Notice of Privacy Practices (NOPPs) discussed in their own PIAs.

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 System of Record Notice (SORN) and Privacy Impact Assessment (PIA) are available for review online. No information is collected directly from individuals and that the source systems have Notice of Privacy Practices (NOPPs) discussed in their own PIAs.

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 opportunity or right to decline to provide information is provided by ABI LAN. No information is collected from the Veteran by ABI LAN. Any opportunity or notice of the right to decline to provide information given to the veteran would be given by the source systems (such as VistA) that collect the information from the Veteran and feed ABI LAN.

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.

Any right to consent to uses of the information would be handled by the source systems that collect the information from the Veteran and feed ABI LAN with information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice from the originating source that their information is being collected, maintained, processed, or disseminated by ABI LAN.

Mitigation: Additional mitigation is provided by making the System of Record Notice (SORN) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1. No information is collected directly from individuals and that the source systems have Notice of Privacy Practices (NOPPs) discussed in their own PIAs.

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.***

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

In addition to the written and published SORNs as listed above, individuals seeking information regarding access to and contesting of records in this system may write or call the VHA Director of National Data Systems (19F4), Austin Information Technology Center (AITC) 1615 Woodward Street, Austin, Texas 78772, or call the VA National Service Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

There are no provisions for correcting inaccurate or erroneous information in ABI LAN. The information in ABI LAN is obtained electronically from VistA and systems interfacing with VistA. Individuals would not gain access to ABI LAN; instead, they would have to go through the source system's protocols to correcting the data.

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 ABI LAN via the feed from VistA.

Mitigation: The information in ABI LAN is obtained via VistA. If there is erroneous or inaccurate information, it should be addressed in the VistA system. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals can 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.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Access to ABI LAN resources is granted to ABI LAN employees, ABI administrative staff, ABI Database administrators, and ABI Management and Program Analysts in accordance with the Office of Analytics and Business Intelligence's (VSSC) Access Request Policy (May 2015).

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?

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.

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.

ABI LAN System enforces PIV for internal users (not including short-term brake/fix solutions). Access to ABI LAN resources is limited to ABI LAN employees. Only ABI administrative staff, ABI Database administrators, and ABI Management and Program Analysis personnel are granted read/write permission, based on their assigned role and in accordance with the Office of Analytics and Business Intelligence's (VSSC) Access Request Policy (May 2015).

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors can be granted access to ABI LAN if their VA manager, COR and system Information System Security Officer (ISSO) approve. They are required to follow the same procedures VA employees do for access, which is to submit a VA Form 9957. They are required to complete annual VA Privacy and Information Security, HIPAA and Rules of Behavior training via the VA's Talent Management System (TMS). In addition, in accordance with the contract between the contractor and the government, all contractors with access to ABI LAN information are required to meet VA contractor security requirements.

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 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS. In addition, ABI LAN has a training portal that provides training via LiveMeeting, self-paced courses, webinars, how-to-guides, monthly user's calls, and newsletters on topics such as navigating the ABI LAN website, using ProClarity tools, subscribing and using reports, and on all Program areas. This portal also has a training calendar that is updated monthly with new training opportunities. ABI LAN users also have access to the ABI LAN Help Desk where they can post questions, problems, or request special access to some of the ABI LAN tools.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approval to Operate is active.
2. *The System Security Plan Status Date:* 28 April 2021
3. *The Authorization Status:* Full ATO granted.
4. *The Authorization Date:* 28 April 2021
5. *The Authorization Termination Date:14 June 2024*
6. *The Risk Review Completion Date:* 04 June 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* The FIPS 199 classification of the system is HIGH.

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

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

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

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.*

KSS does not currently use cloud technology to store PII/PHI.

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.

N/A

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.

N/A

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).

N/A

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 provided in this Privacy Impact Assessment is true and accurate.

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.01.05 08:35:52 -05'00'

Privacy Officer, Kimberly Murphy

JAMES B. ALDEN 201589

Digitally signed by JAMES B. ALDEN 201589
Date: 2023.01.05 15:06:52 -05'00'

Information Systems Security Officer, James Alden

SCOT DINGMAN

Digitally signed by SCOT DINGMAN
Date: 2023.01.17 10:07:19 -06'00'

Information Systems Owner, Scot Dingman

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).

79VA10 – National Patient Databases – VA, and 121VA10A7 – National Patient Databases – VA https://www.oprm.va.gov/docs/SORN/Current_SORN_List_10_21_2022.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