Privacy Impact Assessment for the VA IT System called:

Document Storage System (DSS) Enterprise (DSI)

Veterans Health Administration

Infrastructure Operations

eMASS ID#1771

Date PIA submitted for review:

December 19, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	(503) 721-1037
Information System Security Officer (ISSO)	*Roland Parten*	*Roland.Parten@va.gov*	*(205) 534-6179*
Information System Owner	*Gail Nemetz*	*Gail.Nemetz@va.gov*	*(216) 849-6020*

Abstract

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

DSS applications provide a customized user-friendly Windows Graphical User Interface (GUI) for entering clinical and administrative information that assist with the assessment of ongoing care using current patient data for completed procedures. The DSS programs are applications that use Remote Procedure Call (RPC) Broker, Health Level 7 (HL7), VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies that permit the facility users to store and retrieve clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. DSS Enterprise software is used daily by tens of thousands of clinicians and administrative staff nationwide across various healthcare settings for clinical and administrative users.

Overview

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

1   *General Description*
   A. *What is the IT system name and the name of the program office that owns the IT system?*

      IT System name is Document Storage System (DSS) Enterprise (DSI) and is owned by Infrastructure Operations
   B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

      DSS Enterprise (DSI) applications provide a customized user-friendly Windows Graphical User Interface (GUI) for entering clinical and administrative information that assist with the assessment of ongoing care using current patient data for completed procedures. DSS Enterprise applications record diagnostic findings, including clinical data, charting, and sequenced treatment planning. DSS Enterprise (DSI) applications interface with the Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker, Health Level 7 (HL7), VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies.

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

      IT System owner is Gail Nemetz, Chief COTS Interface Division

2. Information Collection and Sharing
   D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

      DSS Enterprise (DSI) applications are used at all VHA licensed medical centers clinical and administrative personnel (10,000+) which includes healthcare providers and veterans or dependents.

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

DSS Enterprise (DSI) applications consists of several applications (components and minor applications) and the following is the applications general description of the information and purpose:

Components

Above PAR (APAR)	Above PAR (APAR) is a software module for both expendable and non-expendable inventory management. There are two primary modules providing inventory control data and reporting within the VistA Engineering package: Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS) and the Integrated Funds Control and Accountability Package using the Generic Inventory Package (IFCAP GIP) data. APAR is a Graphical User Interface (GUI) that handles Equipment, Inventory, and Work Orders.
Clinical Note Templates (CNT Plus)	CNT Plus supports automatic E&M coding, mandatory and calculable fields, logic algorithms, and Graphics illustrations. The DSS development team customizes templates that VHA medical records committees approve. Full History & Physical Templates by specific practice area and templates by specialty help the facility meets JCAHO & Center for Medicare and Medicaid Services standards. CPRS integrated note generation to assist healthcare providers in meeting compliance for Vera vesting guidelines.
Dental Records Manager Plus (DRM+)	Dental Record Manager Plus (DRM Plus) program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses RPC Broker technology that permits the facility users to store and retrieve clinical data within the VistA System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures.
DSS Enterprise Manager	DSS Enterprise Manager serves as the `administrator` for many DSS applications. This technology performs multiple functions including tracking DSS product inventory on site, facilitating downloads of software updates which DSS distributes every quarter, and allowing authorized users to perform application management functions.
Mental Health Suite (MHS)	Mental Health Suite (MHS) facilitates the development of recovery-based Intake Notes and Interdisciplinary Treatment Plans as Progress Notes and assists clinicians with treating mental health patients. MHS allows clinicians to create, edit, and view treatment plans for an individual patient. MHS allows clinicians to communicate and share case management referral to other medical, psychosocial, and social services. MHS plans are written as a Text Integration Utility (TIU) progress note used in Veterans Health Information Systems & Technology Architecture (VistA) and Computerized Patient Record Systems (CPRS).
Watchdog	DSS Watchdog is a Windows service that can receive preconfigured alerts from VistA along with watching (monitoring) other DSS Windows based services and pass an alert to DSS's Support Works (Help Desk) system via email. Watchdog is used to monitor HL7 (Health Level 7) interfaces between VistA and DSS software applications.
Patient Flow Suite (PFS)	Patient Flow Suite (PFS) is a web platform that connects and maintains interoperability between various Document Storage System (DSS) web-based applications including various services that provide interconnectivity to individual VistA and other VA-hosted services. PFS offers a user a single sign-on experience for any VistA application the user has been given access to via application-specific VistA menu

	options. Once logged into PFS, an authorized user can switch between various DSS web applications that are hosted within PFS while managing the users' VistA menu contexts, offering seamless state management across multiple applications. Currently supported web applications and services in PFS are: Consult Tracking Manager Plus (CTM+), Comprehensive Care Coordination (C3); Order Tracking Manager (Radiology, Lab, Oncology, Dermatology).
Release of Information Plus (ROI Plus)	ROI Plus is a Health Insurance Portability and Accountability Act-compliant software that automates the entire process of managing electronic medical record Release of Information (ROI) requests through the VistA system. It is a proven tool for improving customer experience and employees' workflow efficiencies in processing medical information requests. A Billing module is included that allows Health Information Management Service departments to collect monies for the copies provided above the requestor's allowance.

Minor Applications:

Advanced Prosthetics Acquisition Tool (APAT)	Advanced Prosthetics Acquisition Tool (APAT) automates purchasing workflows and the acquisition of prosthetics, orthotics, and other sensory aids by the Department of Veterans Affairs (VA) medical centers. APAT supports secure electronic document management by helping users scan, index and retrieve purchasing information. APAT enables electronic bid process and purchase order management, provides a color graphical user interface (GUI), tracks comprehensive workflow throughout the process, and allows access to reporting capabilities for ongoing orders.
Comprehensive Care Coordination (C3)	Comprehensive Care Coordination (C3) is a web-based tool that will assist VA staff at any given site to reduce preventable hospitalizations and emergency care for patients with complex medical and social needs. Patients identified as being at the highest risk for unplanned visits, hospitalization, and death. The C3 Dashboard provides patient population information to all applicable VA staff to efficiently identify the highest-risk patients, understand their healthcare histories and socioeconomic realities, and empower the care teams to act on transitional care gaps. Simultaneously, implementing the current programs, technological tools, and resources available to manage the population. In its most basic form, VA medical centers utilizing the application can proactively coordinate holistic care plans, including a patient's social health determinants, and increase their involvement in a patient's care planning beyond the 30-day post-discharge timeframe. The application helps mitigate the risks of incomplete and/or inappropriate coordination activities currently caused by gaps in the transition of care related to reducing readmissions such as high-risk and ACSC diagnoses and medication mismanagement. The application facilitates providing the proper care to the right patient at the right time with the suitable modality of care. C3 is a component of Patient Flow Suite (PFS).
Consult Tracking Manager Plus	Consult Tracking Manager Plus provides a dashboard view of the status of all consults, displayed by service line. The application shows all actions required by role. When a task is complete, it automatically moves through the queue and displays on the next person`s task list as an open item. Consult Tracking Manager Plus is a web-based system interfaced to Veterans Health Information Systems and Technology Architecture (VistA). CTM+ is a component of Patient Flow Suite (PFS).
DocManager VistA Scanning & Indexing System	DocManager is an enterprise-production system to increase the speed and accuracy of document scanning and indexing. Its streamlined workflow process enables personnel to scan (import) documents at designated points (centralized or decentralized stations) in the

	Medical Center, Community-Based Outpatient Clinic, or receive images directly from the fax server. It maximizes facilities' existing scanners and Multi-Function Devices instead of having a printer for each file room clerk. DocMgr indexing functionality automatically closes consults, enables Medical Care Cost Recovery to scan, store, and retrieve Explanation of Benefits (EOB) by receipt and check number, and manage AMMS FISCAL, HR, and other medical center related documents.
Get Well Network (DSIHK)	Get Well Network (GWN) includes patient centered bedside Television, patient education, and room service ordering system. GWN is interfaced with the Computrition system. HL7 interface to VISTA for GWN systems.
Infusion Therapy Manager (ITM)	Infusion Therapy Manager (ITM) is a Web based clinical support tool that is a comprehensive electronic chemotherapy ordering system. ITM is integrated with Vista and provides a framework for evidence-based treatment planning, scheduling, and dosing.
LiveData PeriOp Manager	LiveData PeriOp Manager synchronizes perioperative workflow throughout the entire perioperative suite. PeriOp Manager allows users to coordinate patient flow, patient care, and related resources from preoperative assessment to discharge in real-time. PeriOp Manager allows users to streamline Operating Room (OR) throughput and promotes full compliance with Centers for Medicare and Medicaid Services (CMS), Joint Commission and other critical patient safety mandates. PeriOp Manager Suite connects to VistA, any Anesthesia Record Keeping (ARK) system, physiologic monitor servers or physiological monitoring devices individually.
Order Tracking Manager Radiology (OTM RAD)	Order Tracking Manager Radiology is a web-based application pulling real-time information from VistA for the purpose of assisting staff who have a role with diagnostic imaging. Currently, no systemic approach exists in the VA to ensure the diagnostic reports are seen by the ordering physician nor ability for the ordering provider to easily review, sign complete notes in the patient record. OTM is a component of Patient Flow Suite (PFS).
Iconic Data Patient Case Manager	Patient Case Manager (PCM) is a real-time census management, patient flow optimization, and care coordination platform used by physicians, nurses, discharge planners, bed managers, service line leadership, and facility administrators. The PCM platform is focused on key inpatient clinical and facility operational workflows. The focus is enabling better hospital throughput (improve Veteran access to care), improved patient safety (safer care transitions), and virtual interdisciplinary discharge planning collaboration (reduce length of stay, reduce readmissions). PCM is Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS). This technology stores data in a Microsoft Structured Query Language (SQL) Server database. Suicide Prevention Manager (SPM) is software that assists healthcare clinicians in providing care to patients at high risk for suicide. The technology features data visualization tools, standardized workflows, and analytical tools that work together to monitor processes, performance, and outcomes. Suicide Prevention Manager also monitors patient activities such that case managers, suicide prevention coordinators, and Recovery Engagement and Coordination for Health ` Veterans Enhanced Treatment (REACH VET) coordinators have real time situational awareness when patients may be at risk. The technology utilizes VistA integration to provide real-time information to health workers across mobile and desktop devices. Data collected by this software is stored in a Microsoft Structured Query Language (SQL) Server database.

TheraDoc Infection Surveillance - (COVID related)	TheraDoc enables clinicians within Pharmacy Service and Infection Control to monitor or prevent potential health care risks and provides solutions and means to document interventions that improve clinical outcomes, reduce pharmaceutical expenditures, as well as re-enforce federal and state regulatory compliance. Databases are hosted in Oracle databases and are managed by DSS vendor staff. TheraDoc has a web-based GUI frontend.
VISTA Chemotherapy Manager (VCM)	VCM Automates the clinical practice of Oncology from the assignment of therapy to the calculation of chemotherapy doses through the documentation of care. It combines the range of automation and safety features and flexibility required by Oncology practices. The technology provides a simple user interface and scales to small, medium, and large clinical settings.
VISTA Integrated Revenue Reporting (VIRR)	VIRR is a suite of applications comprised of auditing and claim scrubbing systems for inpatient, outpatient, and professional medical services and is integrated with the VA's designated Encoder software. It has been an essential tool for the Department of Veterans Affairs Medical Centers (VAMCs) by improving productivity and accuracy, reducing medical claim rejections by the payer, and increasing reimbursements. Enterprise Central Reporting provides reports on Key Performance Indicators (KPIs) for tracking revenue workflow and encounter lifecycle at a national level. VIRR uses 3M encoder (standalone version) along with Alpha II CodeWizard tools in VIRR. VistA Integrated Revenue Reporting (VIRR) provides an intelligent, comprehensive approach to VA inpatient and outpatient data management technology for Health Information Management Systems (HIMS), Billing, and Compliance Departments. includes coding and billing modules that aligns hospital and physician coding, reimbursement, and compliance tools to ensure data and coding consistency between physician and facility encounters. There are four modules: Audit Report Manager (ACM), PCE Record Manager (CCM), VIP Director (VIPD) and VIP Workplace (VIPW).
VistA SOA (VSOA)	Veterans Health Information Systems and Technology Architecture (VistA) Service Oriented Architecture (VSOA) Suite is a middleware application development framework built to be compatible with VistA. This technology provides a real-time, bidirectional data and services platform for building and deploying applications with zero downtime. Data is stored in a Microsoft Structured Query Language (SQL) Database. This product can come in two builds: .NET and Node.js-based frameworks. The .NET version runs on the Microsoft Windows platform as a stand-alone service. The Node.js version can be deployed on Linux and macOS based servers. Products using the VSOA technology included in this boundary use the .NET framework.

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

DSS Enterprise (DSI) applications consists of several applications (components and minor applications), and the following information is shared:

Components

Above PAR (APAR)	Above PAR (APAR) is a software module for both expendable and non-expendable inventory management. There are two primary modules providing inventory control data and reporting	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health

	within the VistA Engineering package: Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS) and the Integrated Funds Control and Accountability Package using the Generic Inventory Package (IFCAP GIP) data. APAR is a Graphical User Interface (GUI) that handles Equipment, Inventory, and Work Orders.	Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Clinical Note Templates (CNT Plus)	CNT Plus supports automatic E&M coding, mandatory and calculable fields, logic algorithms, and Graphics illustrations. The DSS development team customizes templates that VHA medical records committees approve. Full History & Physical Templates by specific practice area and templates by specialty help the facility meets JCAHO & Center for Medicare and Medicaid Services standards. CPRS integrated note generation to assist healthcare providers in meeting compliance for Vera vesting guidelines.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Dental Records Manager Plus (DRM+)	Dental Record Manager Plus (DRM Plus) program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses RPC Broker technology that permits the facility users to store and retrieve clinical data within the VistA System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
DSS Enterprise Manager	DSS Enterprise Manager serves as the `administrator` for many DSS applications. This technology performs multiple functions including tracking DSS product inventory on site, facilitating downloads of software updates which DSS distributes every quarter, and allowing authorized users to perform application management functions.	None
Mental Health Suite (MHS)	Mental Health Suite (MHS) facilitates the development of recovery-based Intake Notes and Interdisciplinary Treatment Plans as Progress Notes and assists clinicians with treating mental health patients. MHS allows clinicians to create, edit, and view treatment plans for an individual patient. MHS allows clinicians to communicate and share case management referral to other medical, psychosocial, and social services. MHS plans are written as a Text Integration	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity

	Utility (TIU) progress note used in Veterans Health Information Systems & Technology Architecture (VistA) and Computerized Patient Record Systems (CPRS).	, Gender, Future Appointments, Treatment Plans, Service connected disabilities, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, post Psychiatric History, Military History, Employment History, Financial History.
Watchdog	DSS Watchdog is a Windows service that can receive preconfigured alerts from VistA along with watching (monitoring) other DSS Windows based services and pass an alert to DSS's Support Works (Help Desk) system via email. Watchdog is used to monitor HL7 (Health Level 7) interfaces between VistA and DSS software applications.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Patient Flow Suite (PFS)	Patient Flow Suite (PFS) is a web platform that connects and maintains interoperability between various Document Storage System (DSS) web-based applications including various services that provide interconnectivity to individual VistA and other VA-hosted services. PFS offers a user a single sign-on experience for any VistA application the user has been given access to via application-specific VistA menu options. Once logged into PFS, an authorized user can switch between various DSS web applications that are hosted within PFS while managing the users' VistA menu contexts, offering seamless state management across multiple applications. Currently supported web applications and services in PFS are: Consult Tracking Manager Plus (CTM+), Comprehensive Care Coordination (C3); Order Tracking Manager (Radiology, Lab, Oncology, Dermatology).	Name (Last name, First Name, Middle Initial), VistA DUZ Number, Work-e-mail address,
Release of Information Plus (ROI Plus)	ROI Plus is a Health Insurance Portability and Accountability Act-compliant software that automates the entire process of managing electronic medical record Release of Information (ROI) requests through the VistA system. It is a proven tool for improving customer experience and employees' workflow efficiencies in processing medical information requests. A Billing module is included that allows Health Information Management Service departments to collect monies for the	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic

	copies provided above the requestor's allowance.	name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

Minor Applications:

Advanced Prosthetics Acquisition Tool (APAT)	Advanced Prosthetics Acquisition Tool (APAT) automates purchasing workflows and the acquisition of prosthetics, orthotics, and other sensory aids by the Department of Veterans Affairs (VA) medical centers. APAT supports secure electronic document management by helping users scan, index and retrieve purchasing information. APAT enables electronic bid process and purchase order management, provides a color graphical user interface (GUI), tracks comprehensive workflow throughout the process, and allows access to reporting capabilities for ongoing orders.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Comprehensive Care Coordination (C3)	Comprehensive Care Coordination (C3) is a web-based tool that will assist VA staff at any given site to reduce preventable hospitalizations and emergency care for patients with complex medical and social needs. Patients identified as being at the highest risk for unplanned visits, hospitalization, and death. The C3 Dashboard provides patient population information to all applicable VA staff to efficiently identify the highest-risk patients, understand their healthcare histories and socioeconomic realities, and empower the care teams to act on transitional care gaps. Simultaneously, implementing the current programs, technological tools, and resources available to manage the population. In its most basic form, VA medical centers utilizing the application can proactively coordinate holistic care plans, including a patient's social health determinants, and increase their involvement in a patient's care planning beyond the 30-day post-discharge timeframe. The application helps mitigate the risks of incomplete and/or inappropriate coordination activities currently caused by gaps in the transition of care related to reducing readmissions such as high-risk and ACSC diagnoses and medication mismanagement. The application facilitates providing the proper care to the right patient at the right time with the suitable modality of care. C3 is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

Consult Tracking Manager Plus	Consult Tracking Manager Plus provides a dashboard view of the status of all consults, displayed by service line. The application shows all actions required by role. When a task is complete, it automatically moves through the queue and displays on the next person`s task list as an open item. Consult Tracking Manager Plus is a web-based system interfaced to Veterans Health Information Systems and Technology Architecture (VistA). CTM+ is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
DocManager VistA Scanning & Indexing System	DocManager is an enterprise-production system to increase the speed and accuracy of document scanning and indexing. Its streamlined workflow process enables personnel to scan (import) documents at designated points (centralized or decentralized stations) in the Medical Center, Community-Based Outpatient Clinic, or receive images directly from the fax server. It maximizes facilities' existing scanners and Multi-Function Devices instead of having a printer for each file room clerk. DocMgr indexing functionality automatically closes consults, enables Medical Care Cost Recovery to scan, store, and retrieve Explanation of Benefits (EOB) by receipt and check number, and manage AMMS FISCAL, HR, and other medical center related documents.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
Get Well Network (DSIHK)	Get Well Network (GWN) includes patient centered bedside Television, patient education, and room service ordering system. GWN is interfaced with the Computrition system. HL7 interface to VISTA for GWN systems.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Infusion Therapy Manager (ITM)	Infusion Therapy Manager (ITM) is a Web based clinical support tool that is a comprehensive electronic chemotherapy ordering system. ITM is integrated with Vista and provides a framework for evidence-based treatment planning, scheduling, and dosing.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
LiveData PeriOp Manager	LiveData PeriOp Manager synchronizes perioperative workflow throughout the	Name (Last name, First Name, Middle Initial), SSN, DOB,

	entire perioperative suite. PeriOp Manager allows users to coordinate patient flow, patient care, and related resources from preoperative assessment to discharge in real-time. PeriOp Manager allows users to streamline Operating Room (OR) throughput and promotes full compliance with Centers for Medicare and Medicaid Services (CMS), Joint Commission and other critical patient safety mandates. PeriOp Manager Suite connects to VistA, any Anesthesia Record Keeping (ARK) system, physiologic monitor servers or physiological monitoring devices individually.	Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Vital signs, Surgeries, ADTs,
Order Tracking Manager Radiology (OTM RAD)	Order Tracking Manager Radiology is a web-based application pulling real-time information from VistA for the purpose of assisting staff who have a role with diagnostic imaging. Currently, no systemic approach exists in the VA to ensure the diagnostic reports are seen by the ordering physician nor ability for the ordering provider to easily review, sign complete notes in the patient record. OTM is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.
Iconic Data Patient Case Manager	Patient Case Manager (PCM) is a real-time census management, patient flow optimization, and care coordination platform used by physicians, nurses, discharge planners, bed managers, service line leadership, and facility administrators. The PCM platform is focused on key inpatient clinical and facility operational workflows. The focus is enabling better hospital throughput (improve Veteran access to care), improved patient safety (safer care transitions), and virtual interdisciplinary discharge planning collaboration (reduce length of stay, reduce readmissions). PCM is Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS). This technology stores data in a Microsoft Structured Query Language (SQL) Server database. Suicide Prevention Manager (SPM) is software that assists healthcare clinicians in providing care to patients at high risk for suicide. The technology features data	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity

	visualization tools, standardized workflows, and analytical tools that work together to monitor processes, performance, and outcomes. Suicide Prevention Manager also monitors patient activities such that case managers, suicide prevention coordinators, and Recovery Engagement and Coordination for Health ` Veterans Enhanced Treatment (REACH VET) coordinators have real time situational awareness when patients may be at risk. The technology utilizes VistA integration to provide real-time information to health workers across mobile and desktop devices. Data collected by this software is stored in a Microsoft Structured Query Language (SQL) Server database.	
TheraDoc Infection Surveillance - (COVID related)	TheraDoc enables clinicians within Pharmacy Service and Infection Control to monitor or prevent potential health care risks and provides solutions and means to document interventions that improve clinical outcomes, reduce pharmaceutical expenditures, as well as re-enforce federal and state regulatory compliance. Databases are hosted in Oracle databases and are managed by DSS vendor staff. TheraDoc has a web-based GUI frontend.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Problem List, Attending Provider, allergies, Labs, Surgeries, Admission Discharges and Transfers (ADTs), Radiology results
VISTA Chemotherapy Manager (VCM)	VCM Automates the clinical practice of Oncology from the assignment of therapy to the calculation of chemotherapy doses through the documentation of care. It combines the range of automation and safety features and flexibility required by Oncology practices. The technology provides a simple user interface and scales to small, medium, and large clinical settings.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, ADTs
VISTA Integrated Revenue Reporting (VIRR)	VIRR is a suite of applications comprised of auditing and claim scrubbing systems for inpatient, outpatient, and professional medical services and is integrated with the VA's designated Encoder software. It has been an essential tool for the Department of	Name (Last name, First Name, Middle Initial), SSN, Race/Ethnicity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress

	Veterans Affairs Medical Centers (VAMCs) by improving productivity and accuracy, reducing medical claim rejections by the payer, and increasing reimbursements. Enterprise Central Reporting provides reports on Key Performance Indicators (KPIs) for tracking revenue workflow and encounter lifecycle at a national level. VIRR uses 3M encoder (standalone version) along with Alpha II CodeWizard tools in VIRR. VistA Integrated Revenue Reporting (VIRR) provides an intelligent, comprehensive approach to VA inpatient and outpatient data management technology for Health Information Management Systems (HIMS), Billing, and Compliance Departments. includes coding and billing modules that aligns hospital and physician coding, reimbursement, and compliance tools to ensure data and coding consistency between physician and facility encounters. There are four modules: Audit Report Manager (ACM), PCE Record Manager (CCM), VIP Director (VIPD) and VIP Workplace (VIPW).	notes surgeries, discharge summaries, medications, allergies, date of activity.
VistA SOA (VSOA)	Veterans Health Information Systems and Technology Architecture (VistA) Service Oriented Architecture (VSOA) Suite is a middleware application development framework built to be compatible with VistA. This technology provides a real-time, bidirectional data and services platform for building and deploying applications with zero downtime. Data is stored in a Microsoft Structured Query Language (SQL) Database. This product can come in two builds: .NET and Node.js-based frameworks. The .NET version runs on the Microsoft Windows platform as a stand-alone service. The Node.js version can be deployed on Linux and macOS based servers. Products using the VSOA technology included in this boundary use the .NET framework.	User session log on information (Access Code/Verify Code)

Document Storage System (DSS) Enterprise (DSI) applications are owned by IT Operations and Services (ITOPS), Infrastructure Operations, Veterans Health Administration and the IT System owner is Gail Nemetz, Chief COTS Interface Division. DSS applications provide a customized user-friendly Windows Graphical User Interface (GUI) for entering clinical and administrative information that assist with the assessment of ongoing care using current patient data for completed procedures. DSS Enterprise (DSI) applications interface with the Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker, Health Level 7 (HL7), VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies. DSS Enterprise (DSI) applications provide data input into

the Veterans Health Information Systems and Technology Architecture (VistA) System files such as the Patient Care Encounter (PCE), Text Integration Utility (TIU) and Clinical Patient Record System (CPRS) Problem List packages. DSS Enterprise applications record diagnostic findings, including clinical data, charting, and sequenced treatment planning. DSS Enterprise (DSI) applications help assure quality care, patient safety, and staff communication in an environment that is fully integrated with the VA electronic health record. These applications support the filing of encounters within the guidelines established by the Veterans Health Administration.

DSS Enterprise (DSI) applications use RPC Broker, Health Level 7, VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies which permit the application users to retrieve and store clinical data for active eligible Veterans (over 100,000), dependents, and employees, within the Veterans Health Information Systems and Technology Architecture (VistA) System. Patient Information is retrieved from VistA, (such as – patient's full name (first, middle, and last name), clinic name/location, visit date, and medical records information such as medication, health summaries, lab, consults, and imaging). The DSS Enterprise (DSI) diagnostic information, coding, and crediting procedures, and progress notes (TIU (Text Integration Utilities)) are saved in VistA and diagnostic images are saved in the VistA Imaging System.

The use of DSS Enterprise (DSI) applications result in more accurate insurance billing for visits, consults and procedures. The applications support the filing within the guidelines established by the Veterans Health Administration.

DSS Enterprise (DSI) applications are used at all VHA licensed sites, and the software is hosted several different ways. Most of the applications related to healthcare or health administration will have a scope within OI&T Regions 1 through 4. For the purposes of this document, any application with a scope outside of Regions 1 through 4 will be considered National in scope.

•Site - Applications in this scope provide a service to a specific site, which could be a VA medical center or outpatient clinic. Applications with a Site scope will have one complete and independent system for each Site in a Region.

•VISN – Applications in this scope provide a service at a VISN level. The data and business owners are affiliated with all sites within the VISN while the system owners remain Regional. Applications with a VISN scope will have one complete and independent system for each VISN in a Region.

Some VISN servers may still have Site-specific databases, folders, or shares, but the system itself is considered VISN-centric.

•Regional – Applications in this scope provide a service at a Regional level. The data, system, and business owners are affiliated with all sites in all VISNs within the Region. Applications with a Regional scope will have four complete and independent systems; one for each of the Regions supporting VHA hospitals and clinics. Some Regional servers may still have VISN-specific databases, folders, OI&T shares, but the system itself is considered Region-centric.

•National – Applications in this scope provide a service at a National level. The data, system, and business owners are not affiliated with a particular hospital, VISN, or Region. Applications in this scope are configured

and managed at the National level. While some parts of the application may run on servers with smaller application scopes, they are still considered Nation-centric.

The VA considers DSS Enterprise (DSI) applications to be COTS products because they could be sold and interfaced with other systems. The completion of the PIA will not change the business and technology processes.

DSS Enterprise (DSI)'s legal authority for operating: Title 38, United States Code, Sections 501(b) and 304. The applicable System of Records Notices (SORN) are 24VA10A7, Patient Medical Record-VA, 121VA10A7, National Patient Databases-VA, and 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA.

Components of the Major/Parent boundary:

Above PAR (APAR)
Clinical Note Templates (CNT Plus)
Dental Records Manager Plus (DRM Plus)
Enterprise Manager
Mental Health Suite (MHS)
Patient Flow Suite (PFS)
Release of Information Plus (ROI Plus)
Watchdog

Minor applications:

Advanced Prosthetics Acquisition Tool (APAT) – eMASS 2075
Comprehensive Care Coordination (C3) – eMASS 2229
Consult Tracking Manager Plus (CTM Plus) – eMASS 2041
DocManager VistA Scanning & Indexing System (DocManager) – eMASS 2260
Get Well Network (DSIHK) – eMASS 2246
Infusion Therapy Manager (ITM) – eMASS 2352
LiveData PeriOp Manager (DSIHL) – eMASS 2230
Order Tracking Manager Radiology (OTM RAD) – eMASS 2273
Iconic Data Patient Case Manager – eMASS ID pending
TheraDoc Infection Surveillance - (COVID related) – eMASS 2169
VISTA Chemotherapy Manager (VCM) – eMASS 2223
VISTA Integrated Revenue Reporting (VIRR) – eMASS 2275
VistA SOA (VSOA) – eMASS 2076

Below is a table with descriptions of how the components and minor applications of this system use information:

Components

Above PAR (APAR)	Above PAR (APAR) is a software module for both expendable and non-expendable inventory management. There are two primary modules providing inventory control data and reporting within the VistA Engineering package: Automated Engineering Management	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current

	System/Medical Equipment Reporting System (AEMS/MERS) and the Integrated Funds Control and Accountability Package using the Generic Inventory Package (IFCAP GIP) data. APAR is a Graphical User Interface (GUI) that handles Equipment, Inventory, and Work Orders.	Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Clinical Note Templates (CNT Plus)	CNT Plus supports automatic E&M coding, mandatory and calculable fields, logic algorithms, and Graphics illustrations. The DSS development team customizes templates that VHA medical records committees approve. Full History & Physical Templates by specific practice area and templates by specialty help the facility meets JCAHO & Center for Medicare and Medicaid Services standards. CPRS integrated note generation to assist healthcare providers in meeting compliance for Vera vesting guidelines.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Dental Records Manager Plus (DRM+)	Dental Record Manager Plus (DRM Plus) program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses RPC Broker technology that permits the facility users to store and retrieve clinical data within the VistA System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
DSS Enterprise Manager	DSS Enterprise Manager serves as the `administrator` for many DSS applications. This technology performs multiple functions including tracking DSS product inventory on site, facilitating downloads of software updates which DSS distributes every quarter, and allowing authorized users to perform application management functions.	None
Mental Health Suite (MHS)	Mental Health Suite (MHS) facilitates the development of recovery-based Intake Notes and Interdisciplinary Treatment Plans as Progress Notes and assists clinicians with treating mental health patients. MHS allows clinicians to create, edit, and view treatment plans for an individual patient. MHS allows clinicians to communicate and share case management referral to other medical, psychosocial, and social services. MHS plans are written as a Text Integration Utility (TIU) progress note used in Veterans Health Information Systems &	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity , Gender, Future Appointments, Treatment Plans, Service

	Technology Architecture (VistA) and Computerized Patient Record Systems (CPRS).	connected disabilities, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, post Psychiatric History, Military History, Employment History, Financial History.
Watchdog	DSS Watchdog is a Windows service that can receive preconfigured alerts from VistA along with watching (monitoring) other DSS Windows based services and pass an alert to DSS's Support Works (Help Desk) system via email. Watchdog is used to monitor HL7 (Health Level 7) interfaces between VistA and DSS software applications.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Patient Flow Suite (PFS)	Patient Flow Suite (PFS) is a web platform that connects and maintains interoperability between various Document Storage System (DSS) web-based applications including various services that provide interconnectivity to individual VistA and other VA-hosted services. PFS offers a user a single sign-on experience for any VistA application the user has been given access to via application-specific VistA menu options. Once logged into PFS, an authorized user can switch between various DSS web applications that are hosted within PFS while managing the users' VistA menu contexts, offering seamless state management across multiple applications. Currently supported web applications and services in PFS are: Consult Tracking Manager Plus (CTM+), Comprehensive Care Coordination (C3); Order Tracking Manager (Radiology, Lab, Oncology, Dermatology).	Name (Last name, First Name, Middle Initial), VistA DUZ Number, Work-e-mail address,
Release of Information Plus (ROI Plus)	ROI Plus is a Health Insurance Portability and Accountability Act-compliant software that automates the entire process of managing electronic medical record Release of Information (ROI) requests through the VistA system. It is a proven tool for improving customer experience and employees' workflow efficiencies in processing medical information requests. A Billing module is included that allows Health Information Management Service departments to collect monies for the copies provided above the requestor's allowance.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress

		notes surgeries, discharge summaries, medications, allergies, date of activity.

Minor Applications

Advanced Prosthetics Acquisition Tool (APAT)	Advanced Prosthetics Acquisition Tool (APAT) automates purchasing workflows and the acquisition of prosthetics, orthotics, and other sensory aids by the Department of Veterans Affairs (VA) medical centers. APAT supports secure electronic document management by helping users scan, index and retrieve purchasing information. APAT enables electronic bid process and purchase order management, provides a color graphical user interface (GUI), tracks comprehensive workflow throughout the process, and allows access to reporting capabilities for ongoing orders.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Comprehensive Care Coordination (C3)	Comprehensive Care Coordination (C3) is a web-based tool that will assist VA staff at any given site to reduce preventable hospitalizations and emergency care for patients with complex medical and social needs. Patients identified as being at the highest risk for unplanned visits, hospitalization, and death. The C3 Dashboard provides patient population information to all applicable VA staff to efficiently identify the highest-risk patients, understand their healthcare histories and socioeconomic realities, and empower the care teams to act on transitional care gaps. Simultaneously, implementing the current programs, technological tools, and resources available to manage the population. In its most basic form, VA medical centers utilizing the application can proactively coordinate holistic care plans, including a patient's social health determinants, and increase their involvement in a patient's care planning beyond the 30-day post-discharge timeframe. The application helps mitigate the risks of incomplete and/or inappropriate coordination activities currently caused by gaps in the transition of care related to reducing readmissions such as high-risk and ACSC diagnoses and medication mismanagement. The application facilitates providing the proper care to the right patient at the right time with the suitable modality of	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

	care. C3 is a component of Patient Flow Suite (PFS).	
Consult Tracking Manager Plus	Consult Tracking Manager Plus provides a dashboard view of the status of all consults, displayed by service line. The application shows all actions required by role. When a task is complete, it automatically moves through the queue and displays on the next person`s task list as an open item. Consult Tracking Manager Plus is a web-based system interfaced to Veterans Health Information Systems and Technology Architecture (VistA). CTM+ is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
DocManager VistA Scanning & Indexing System	DocManager is an enterprise-production system to increase the speed and accuracy of document scanning and indexing. Its streamlined workflow process enables personnel to scan (import) documents at designated points (centralized or decentralized stations) in the Medical Center, Community-Based Outpatient Clinic, or receive images directly from the fax server. It maximizes facilities' existing scanners and Multi-Function Devices instead of having a printer for each file room clerk. DocMgr indexing functionality automatically closes consults, enables Medical Care Cost Recovery to scan, store, and retrieve Explanation of Benefits (EOB) by receipt and check number, and manage AMMS FISCAL, HR, and other medical center related documents.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
Get Well Network (DSIHK)	Get Well Network (GWN) includes patient centered bedside Television, patient education, and room service ordering system. GWN is interfaced with the Computrition system. HL7 interface to VISTA for GWN systems.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Infusion Therapy Manager (ITM)	Infusion Therapy Manager (ITM) is a Web based clinical support tool that is a comprehensive electronic chemotherapy ordering system. ITM is integrated with Vista and provides a framework for evidence-based treatment planning, scheduling, and dosing.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity

LiveData PeriOp Manager	LiveData PeriOp Manager synchronizes perioperative workflow throughout the entire perioperative suite. PeriOp Manager allows users to coordinate patient flow, patient care, and related resources from preoperative assessment to discharge in real-time. PeriOp Manager allows users to streamline Operating Room (OR) throughput and promotes full compliance with Centers for Medicare and Medicaid Services (CMS), Joint Commission and other critical patient safety mandates. PeriOp Manager Suite connects to VistA, any Anesthesia Record Keeping (ARK) system, physiologic monitor servers or physiological monitoring devices individually.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Vital signs, Surgeries, ADTs,
Order Tracking Manager Radiology (OTM RAD)	Order Tracking Manager Radiology is a web-based application pulling real-time information from VistA for the purpose of assisting staff who have a role with diagnostic imaging. Currently, no systemic approach exists in the VA to ensure the diagnostic reports are seen by the ordering physician nor ability for the ordering provider to easily review, sign complete notes in the patient record. OTM is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.
Iconic Data Patient Case Manager	Patient Case Manager (PCM) is a real-time census management, patient flow optimization, and care coordination platform used by physicians, nurses, discharge planners, bed managers, service line leadership, and facility administrators. The PCM platform is focused on key inpatient clinical and facility operational workflows. The focus is enabling better hospital throughput (improve Veteran access to care), improved patient safety (safer care transitions), and virtual interdisciplinary discharge planning collaboration (reduce length of stay, reduce readmissions). PCM is Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS). This technology stores data in a Microsoft Structured Query Language (SQL) Server database. Suicide Prevention Manager (SPM) is software that assists healthcare clinicians	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity

	in providing care to patients at high risk for suicide. The technology features data visualization tools, standardized workflows, and analytical tools that work together to monitor processes, performance, and outcomes. Suicide Prevention Manager also monitors patient activities such that case managers, suicide prevention coordinators, and Recovery Engagement and Coordination for Health ` Veterans Enhanced Treatment (REACH VET) coordinators have real time situational awareness when patients may be at risk. The technology utilizes VistA integration to provide real-time information to health workers across mobile and desktop devices. Data collected by this software is stored in a Microsoft Structured Query Language (SQL) Server database.	
TheraDoc Infection Surveillance - (COVID related)	TheraDoc enables clinicians within Pharmacy Service and Infection Control to monitor or prevent potential health care risks and provides solutions and means to document interventions that improve clinical outcomes, reduce pharmaceutical expenditures, as well as re-enforce federal and state regulatory compliance. Databases are hosted in Oracle databases and are managed by DSS vendor staff. TheraDoc has a web-based GUI frontend.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Problem List, Attending Provider, allergies, Labs, Surgeries, Admission Discharges and Transfers (ADTs), Radiology results
VISTA Chemotherapy Manager (VCM)	VCM Automates the clinical practice of Oncology from the assignment of therapy to the calculation of chemotherapy doses through the documentation of care. It combines the range of automation and safety features and flexibility required by Oncology practices. The technology provides a simple user interface and scales to small, medium, and large clinical settings.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, ADTs
VISTA Integrated Revenue Reporting (VIRR)	VIRR is a suite of applications comprised of auditing and claim scrubbing systems for inpatient, outpatient, and professional medical services and is integrated with the VA's	Name (Last name, First Name, Middle Initial), SSN, Race/Ethnicity, current and previous medical records information such as clinic

	designated Encoder software. It has been an essential tool for the Department of Veterans Affairs Medical Centers (VAMCs) by improving productivity and accuracy, reducing medical claim rejections by the payer, and increasing reimbursements. Enterprise Central Reporting provides reports on Key Performance Indicators (KPIs) for tracking revenue workflow and encounter lifecycle at a national level. VIRR uses 3M encoder (standalone version) along with Alpha II CodeWizard tools in VIRR. VistA Integrated Revenue Reporting (VIRR) provides an intelligent, comprehensive approach to VA inpatient and outpatient data management technology for Health Information Management Systems (HIMS), Billing, and Compliance Departments. includes coding and billing modules that aligns hospital and physician coding, reimbursement, and compliance tools to ensure data and coding consistency between physician and facility encounters. There are four modules: Audit Report Manager (ACM), PCE Record Manager (CCM), VIP Director (VIPD) and VIP Workplace (VIPW).	name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.
VistA SOA (VSOA)	Veterans Health Information Systems and Technology Architecture (VistA) Service Oriented Architecture (VSOA) Suite is a middleware application development framework built to be compatible with VistA. This technology provides a real-time, bidirectional data and services platform for building and deploying applications with zero downtime. Data is stored in a Microsoft Structured Query Language (SQL) Database. This product can come in two builds: .NET and Node.js-based frameworks. The .NET version runs on the Microsoft Windows platform as a stand-alone service. The Node.js version can be deployed on Linux and macOS based servers. Products using the VSOA technology included in this boundary use the .NET framework.	User session log on information (Access Code/Verify Code)

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

DSS Enterprise (DSI) applications are used at all VHA licensed sites, and the software is hosted several different ways. Most of the applications related to healthcare or health administration

will have a scope within OI&T Regions 1 through 4. For the purposes of this document, any application with a scope outside of Regions 1 through 4 will be considered National in scope.

• Site - Applications in this scope provide a service to a specific site, which could be a VA medical center or outpatient clinic. Applications with a Site scope will have one complete and independent system for each Site in a Region.
• VISN – Applications in this scope provide a service at a VISN level. The data and business owners are affiliated with all sites within the VISN while the system owners remain Regional. Applications with a VISN scope will have one complete and independent system for each VISN in a Region. Some VISN servers may still have Site-specific databases, folders, or shares, but the system itself is considered VISN-centric.
• Regional – Applications in this scope provide a service at a Regional level. The data, system, and business owners are affiliated with all sites in all VISNs within the Region. Applications with a Regional scope will have four complete and independent systems; one for each of the Regions supporting VHA hospitals and clinics. Some Regional servers may still have VISN-specific databases, folders, or shares, but the system itself is considered Region-centric.
• National – Applications in this scope provide a service at a National level. The data, system, and business owners are not affiliated with a particular hospital, VISN, or Region. Applications in this scope are configured and managed at the National level. While some parts of the application may run on servers with smaller application scopes, they are still considered Nation-centric.

3. Legal Authority and SORN
    H. What is the citation of the legal authority to operate the IT system?

DSS Enterprise (DSI)'s legal authorities for operating the system are found in the SORNS that apply to the particular component or minor system:

Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

Patient Medical Record – VA, SORN 24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

National Patient Databases – VA, SORN 121VA10 https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501.

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

These systems are not in the process of being modified nor is it using cloud technology.

4. System Changes

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

No changes are required.

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

No changes are required.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)

☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information

☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers

---

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

☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification
Number
☒ Medical Record
Number
☒ Gender

☒ Integrated Control
Number (ICN)
☐ Military
History/Service
Connection
☒ Next of Kin
☒ Other Data Elements
(list below)

Other PII/PHI data elements:
Account Numbers
Problem List
Attending Provider
Allergies
Laboratory Results
Surgeries
Admission Discharges and Transfers (ADTs)
Radiology Results
Vital Signs
Network Accounts Information
Date of Activity

PII Mapping of Components (Servers/Database)

DSS Enterprise (DSI) consists of component and minor applications; and each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DSS Enterprise (DSI) and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Veterans Health Information Systems and Technology Architecture (VistA)/VistA VAEC) Components/ Applications connect to the VistA database at any given datacenter (AITC, PITC)	Yes	Yes	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health	Ensure correct record is retrieve from VistA	Data is encrypted

			Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity		
Veterans Health Information Systems and Technology Architecture (VistA) Imaging System	Yes	Yes	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.	Update patient record	Behind an MDIA, Uses access and verify code for authentication, and retention history
Computrition	Yes	Yes	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address;	Ensures meals are delivered to the correct patient and ensures food allergies are reviewed.	Data is encrypted

			Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity		
Coding and Reimbursement System Plus	No	No	Admission date, discharge date, age	N/A	Only displays data, no fields can be modified
Bio-Med - ClinComp	Yes	Yes	User session log on information (Access Code/Verify Code)	Contains patient data required for surgery information; e.g., vitals, ADTs, medical information	Behind MDIA

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?

DSS Enterprise (DSI) information is collected by all VHA licensed medical centers clinical and administrative personnel which includes healthcare providers, veterans or dependents and other vendor's applications to provide clinical and administrative information that assist with the assessment of ongoing care using current patient data for completed procedures.

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.

DSS Enterprise (DSI) applications does not use data from a commercial aggregator of information or is data taken from the public website(s).

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

DSS Enterprise (DSI) applications use RPC Broker, Health Level 7 (HL7), VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies which permit the application end users to retrieve and store clinical and administrative data within the Veterans Health Information Systems and Technology Architecture (VistA) System. The DSS Enterprise (DSI)

diagnostic information, coding and crediting, progress notes (TIU (Text Integration Utilities)) are saved in VistA and diagnostic images are saved in the VistA Imaging System.

The following lists DSS, Inc products included in the DSS Enterprise ATO boundary.

Above PAR (APAR)	Above PAR (APAR) is a software module for both expendable and non-expendable inventory management. There are two primary modules providing inventory control data and reporting within the VistA Engineering package: Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS`) and the Integrated Funds Control and Accountability Package using the Generic Inventory Package (IFCAP GIP) data. APAR is a Graphical User Interface (GUI) that handles Equipment, Inventory, and Work Orders.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Clinical Note Templates (CNT Plus)	CNT Plus supports automatic E&M coding, mandatory and calculable fields, logic algorithms, and Graphics illustrations. The DSS development team customizes templates that VHA medical records committees approve. Full History & Physical Templates by specific practice area and templates by specialty help the facility meets JCAHO & Center for Medicare and Medicaid Services standards. CPRS integrated note generation to assist healthcare providers in meeting compliance for Vera vesting guidelines.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Dental Records Manager Plus (DRM+)	Dental Record Manager Plus (DRM Plus) program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses RPC Broker technology that permits the facility users to store and retrieve clinical data within the VistA System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
DSS Enterprise Manager	DSS Enterprise Manager serves as the `administrator` for many DSS applications. This technology performs multiple functions including tracking DSS product inventory on site, facilitating downloads of software	None

	updates which DSS distributes every quarter, and allowing authorized users to perform application management functions.	
Mental Health Suite (MHS)	Mental Health Suite (MHS) facilitates the development of recovery-based Intake Notes and Interdisciplinary Treatment Plans as Progress Notes and assists clinicians with treating mental health patients. MHS allows clinicians to create, edit, and view treatment plans for an individual patient. MHS allows clinicians to communicate and share case management referral to other medical, psychosocial, and social services. MHS plans are written as a Text Integration Utility (TIU) progress note used in Veterans Health Information Systems & Technology Architecture (VistA) and Computerized Patient Record Systems (CPRS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity , Gender, Future Appointments, Treatment Plans, Service connected disabilities, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, post Psychiatric History, Military History, Employment History, Financial History.
Watchdog	DSS Watchdog is a Windows service that can receive preconfigured alerts from VistA along with watching (monitoring) other DSS Windows based services and pass an alert to DSS's Support Works (Help Desk) system via email. Watchdog is used to monitor HL7 (Health Level 7) interfaces between VistA and DSS software applications.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Patient Flow Suite (PFS)	Patient Flow Suite (PFS) is a web platform that connects and maintains interoperability between various Document Storage System (DSS) web-based applications including various services that provide interconnectivity to individual VistA and other VA-hosted services. PFS offers a user a single sign-on experience for any VistA application the user has been given access to via application-specific VistA menu options. Once logged into PFS, an authorized user can switch between various DSS web applications that are hosted within PFS while managing the users' VistA menu contexts, offering seamless state management across multiple applications. Currently	Name (Last name, First Name, Middle Initial), VistA DUZ Number, Work-e-mail address,

	supported web applications and services in PFS are: Consult Tracking Manager Plus (CTM+), Comprehensive Care Coordination (C3); Order Tracking Manager (Radiology, Lab, Oncology, Dermatology).	
Release of Information Plus (ROI Plus)	ROI Plus is a Health Insurance Portability and Accountability Act-compliant software that automates the entire process of managing electronic medical record Release of Information (ROI) requests through the VistA system. It is a proven tool for improving customer experience and employees' workflow efficiencies in processing medical information requests. A Billing module is included that allows Health Information Management Service departments to collect monies for the copies provided above the requestor's allowance.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

Advanced Prosthetics Acquisition Tool (APAT)	Advanced Prosthetics Acquisition Tool (APAT) automates purchasing workflows and the acquisition of prosthetics, orthotics, and other sensory aids by the Department of Veterans Affairs (VA) medical centers. APAT supports secure electronic document management by helping users scan, index and retrieve purchasing information. APAT enables electronic bid process and purchase order management, provides a color graphical user interface (GUI), tracks comprehensive workflow throughout the process, and allows access to reporting capabilities for ongoing orders.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Comprehensive Care Coordination (C3)	Comprehensive Care Coordination (C3) is a web-based tool that will assist VA staff at any given site to reduce preventable hospitalizations and emergency care for patients with complex medical and social needs. Patients identified as being at the highest risk for unplanned visits, hospitalization, and death. The C3 Dashboard provides patient population information to all applicable VA staff to efficiently identify the highest-risk patients, understand their healthcare histories and socioeconomic realities, and empower the care teams to act on transitional care gaps. Simultaneously, implementing the current programs,	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult,

	technological tools, and resources available to manage the population. In its most basic form, VA medical centers utilizing the application can proactively coordinate holistic care plans, including a patient's social health determinants, and increase their involvement in a patient's care planning beyond the 30-day post-discharge timeframe. The application helps mitigate the risks of incomplete and/or inappropriate coordination activities currently caused by gaps in the transition of care related to reducing readmissions such as high-risk and ACSC diagnoses and medication mismanagement. The application facilitates providing the proper care to the right patient at the right time with the suitable modality of care. C3 is a component of Patient Flow Suite (PFS).	imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.
Consult Tracking Manager Plus	Consult Tracking Manager Plus provides a dashboard view of the status of all consults, displayed by service line. The application shows all actions required by role. When a task is complete, it automatically moves through the queue and displays on the next person`s task list as an open item. Consult Tracking Manager Plus is a web-based system interfaced to Veterans Health Information Systems and Technology Architecture (VistA). CTM+ is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
DocManager VistA Scanning & Indexing System	DocManager is an enterprise-production system to increase the speed and accuracy of document scanning and indexing. Its streamlined workflow process enables personnel to scan (import) documents at designated points (centralized or decentralized stations) in the Medical Center, Community-Based Outpatient Clinic, or receive images directly from the fax server. It maximizes facilities' existing scanners and Multi-Function Devices instead of having a printer for each file room clerk. DocMgr indexing functionality automatically closes consults, enables Medical Care Cost Recovery to scan, store, and retrieve Explanation of Benefits (EOB) by receipt and check number, and manage AMMS FISCAL, HR, and other medical center related documents.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Race/Ethnicity; Gender, Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity, network accounts
Get Well Network (DSIHK)	Get Well Network (GWN) includes patient centered bedside Television, patient education, and room service	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address;

	ordering system. GWN is interfaced with the Computrition system. HL7 interface to VISTA for GWN systems.	Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
Infusion Therapy Manager (ITM)	Infusion Therapy Manager (ITM) is a Web based clinical support tool that is a comprehensive electronic chemotherapy ordering system. ITM is integrated with Vista and provides a framework for evidence-based treatment planning, scheduling, and dosing.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity
LiveData PeriOp Manager	LiveData PeriOp Manager synchronizes perioperative workflow throughout the entire perioperative suite. PeriOp Manager allows users to coordinate patient flow, patient care, and related resources from preoperative assessment to discharge in real-time. PeriOp Manager allows users to streamline Operating Room (OR) throughput and promotes full compliance with Centers for Medicare and Medicaid Services (CMS), Joint Commission and other critical patient safety mandates. PeriOp Manager Suite connects to VistA, any Anesthesia Record Keeping (ARK) system, physiologic monitor servers or physiological monitoring devices individually.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Vital signs, Surgeries, ADTs,
Order Tracking Manager Radiology (OTM RAD)	Order Tracking Manager Radiology is a web-based application pulling real-time information from VistA for the purpose of assisting staff who have a role with diagnostic imaging. Currently, no systemic approach exists in the VA to ensure the diagnostic reports are seen by the ordering physician nor ability for the ordering provider to easily review, sign complete notes in the patient record. OTM is a component of Patient Flow Suite (PFS).	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult,

		imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.
Iconic Data Patient Case Manager	Patient Case Manager (PCM) is a real-time census management, patient flow optimization, and care coordination platform used by physicians, nurses, discharge planners, bed managers, service line leadership, and facility administrators. The PCM platform is focused on key inpatient clinical and facility operational workflows. The focus is enabling better hospital throughput (improve Veteran access to care), improved patient safety (safer care transitions), and virtual interdisciplinary discharge planning collaboration (reduce length of stay, reduce readmissions). PCM is Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS). This technology stores data in a Microsoft Structured Query Language (SQL) Server database.

Suicide Prevention Manager (SPM) is software that assists healthcare clinicians in providing care to patients at high risk for suicide. The technology features data visualization tools, standardized workflows, and analytical tools that work together to monitor processes, performance, and outcomes. Suicide Prevention Manager also monitors patient activities such that case managers, suicide prevention coordinators, and Recovery Engagement and Coordination for Health ` Veterans Enhanced Treatment (REACH VET) coordinators have real time situational awareness when patients may be at risk. The technology utilizes VistA integration to provide real-time information to health workers across mobile and desktop devices. Data collected by this software is stored in a Microsoft Structured Query Language (SQL) Server database. | Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity |
| TheraDoc Infection Surveillance - (COVID related) | TheraDoc enables clinicians within Pharmacy Service and Infection Control to monitor or prevent potential health care risks and provides solutions and means to document interventions that improve clinical outcomes, reduce pharmaceutical | Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); |

	expenditures, as well as re-enforce federal and state regulatory compliance. Databases are hosted in Oracle databases and are managed by DSS vendor staff. TheraDoc has a web-based GUI frontend.	Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, Problem List, Attending Provider, allergies, Labs, Surgeries, Admission Discharges and Transfers (ADTs), Radiology results
VISTA Chemotherapy Manager (VCM)	VCM Automates the clinical practice of Oncology from the assignment of therapy to the calculation of chemotherapy doses through the documentation of care. It combines the range of automation and safety features and flexibility required by Oncology practices. The technology provides a simple user interface and scales to small, medium, and large clinical settings.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, ADTs
VISTA Integrated Revenue Reporting (VIRR)	VIRR is a suite of applications comprised of auditing and claim scrubbing systems for inpatient, outpatient, and professional medical services and is integrated with the VA's designated Encoder software. It has been an essential tool for the Department of Veterans Affairs Medical Centers (VAMCs) by improving productivity and accuracy, reducing medical claim rejections by the payer, and increasing reimbursements. Enterprise Central Reporting provides reports on Key Performance Indicators (KPIs) for tracking revenue workflow and encounter lifecycle at a national level. VIRR uses 3M encoder (standalone version) along with Alpha II CodeWizard tools in VIRR. VistA Integrated Revenue Reporting (VIRR) provides an intelligent, comprehensive approach to VA inpatient and outpatient data management technology for Health Information Management Systems (HIMS), Billing, and Compliance Departments. includes coding and billing modules that aligns hospital and physician coding, reimbursement, and compliance tools to ensure data and coding consistency between physician	Name (Last name, First Name, Middle Initial), SSN, Race/Ethnicity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

	and facility encounters. There are four modules: Audit Report Manager (ACM), PCE Record Manager (CCM), VIP Director (VIPD) and VIP Workplace (VIPW).	
VistA SOA (VSOA)	Veterans Health Information Systems and Technology Architecture (VistA) Service Oriented Architecture (VSOA) Suite is a middleware application development framework built to be compatible with VistA. This technology provides a real-time, bidirectional data and services platform for building and deploying applications with zero downtime. Data is stored in a Microsoft Structured Query Language (SQL) Database. This product can come in two builds: .NET and Node.js-based frameworks. The .NET version runs on the Microsoft Windows platform as a stand-alone service. The Node.js version can be deployed on Linux and macOS based servers. Products using the VSOA technology included in this boundary use the .NET framework.	User session log on information (Access Code/Verify Code)

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?

Directly from individual, received via electronic transmission from other systems, and/or also created by the system itself. Other application(s) could receive patient records from third party healthcare providers and requires scanning into the VistA system.

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

 DSS Enterprise (DSI) information is not collected on a form and is not subject to the Paperwork Reduction Act.

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

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

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

Some of the DSS Enterprise (DSI) applications are Graphical User Interface (GUI) front-end for data input into the Veterans Health Information Systems and Technology Architecture (VistA), patient files as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU), Computerized Patient Record Search (CPRS) Problem List, and Vitals packages. This technology allows doctors and staff to access a patient`s entire medical record and enables them to enter diagnostic findings, treatment plan procedures and patient-specific notes into the patient`s Electronic Health Record. Application users require a VistA account with CPRS VistA secondary menu option/security key/VistA Person Class Code, etc. to retrieve and store new data.

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

DSS Enterprise (DSI) does not check for accuracy by accessing a commercial aggregator of information.

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 38 United States Code (U.S.C.) §§1701, 1703, 1710(c), 1712, 3104 and Title 38 Code of Federal Regulation (CFR) Chapter 17 authorizes the provision of Veterans medical, nursing home, and domiciliary care and associated record-keeping.

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

SORN 24VA10A7 "Patient Medical Record-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

SORN 121VA10 "National Patient Databases-VA", https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501.

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 DSS Enterprise (DSI) applications retrieve and collect Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the Veteran in crisis, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the Veterans' information. Users are trained on how to handle sensitive information by taking VA Privacy and Security Awareness Training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name (Last name, First Name, Middle Initial)	Used as a person's identifier	Not used
SSN	Assists in uniquely identifying the person's medical record.	Not used
Date Of Birth	Assists to identify patient age and confirm patient identity	Not used
Personal Mailing Address	Used to contact the individual	Not used
Personal Phone Number(s)	Used to contact the individual	Not used
Personal e-mail Address	Used to contact the individual	Not used
Emergency Contact Information	Used to contact next of kin in an emergency	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used to file claims	Not used
Current Medications	Assists to determine medical history and healthcare outcome and used to administer medication	Not used
Previous Medical Records	Assists to determine medical history and healthcare outcome	Not used
Race/Ethnicity	Assists to determine Race/Ethnicity.	Not used
Medical Record Number	Assists in uniquely identifying the person's medical record	Not used
Other Unique Identifying Number (ICN Internal Control Number)	Assists in uniquely identifying the person's medical record	Not used
Date of activity	Used to identify the date/time of visit. Included in the TIU note.	Not used
Problem List	Identification of patient diagnosis	Not used
Attending Provider	Identification of medical professional assigned	Not used
Allergies	Used to describe patient medical adverse reactions.	Not used

Laboratory Results	Used as patient medical care	Not used
Surgeries	Used as patient medical care	Not used
Admission Discharges and Transfers (ADTs)	Automated patient movements	Not used
Radiology Results	Used as patient medical care	Not used
Vital Signs	Used as patient medical care	Not used
Network Accounts Information	Used to identify specific employee(s)	Not used
Employee e-mail	Used to contact the individual	Not used
VistA DUZ Number	Used to identify specific employee(s)	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

VA issues guidelines maximizing the objectivity of disseminated Privacy Act information in VA Directive 6502. VA issues guidelines maximizing the objectivity of disseminated Privacy Act information in VA Directive 0009. VA Privacy Service establishes in VA Directive 6502, p. 7 that: '(2) To the greatest extent practicable, the PII is collected directly from the individual to whom it pertains; and '(3) When it is not possible to collect PII directly from the individual and that information is collected from third parties, it will be verified with the subject of the record to the greatest extent practicable before any negative action is taken. The VA defines the frequency on which it will check for, and correct as necessary, inaccurate, or outdated PII used by its programs or systems as 'continuously, and as needed. VA issues guidelines ensuring the quality of disseminated Privacy Act information in VA Directive 0009. VA issues guidelines ensuring the utility of disseminated Privacy Act information in VA Directive 0009.   VA issues guidelines maximizing the objectivity of disseminated Privacy Act information in VA Directive 0009.

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.
DSS Enterprise (DSI) applications do not analyze or produce patient data. These programs are designed to provide health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient medical conditions, and develop and maintain the treatment plans. The DSS Enterprise (DSI) programs are applications that use RPC Broker,

Health Level 7, VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System technologies which permit the facility users to store and retrieve clinical data within the VistA System. Each DSS Enterprise (DSI) application require application-specific VistA menu option(s) and/or VistA security key(s) to retrieve, create, and store data in VistA.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Data is encrypted when it resides in VistA. Social Security Numbers are often abbreviated to give added protection. The hard drives that the applications/databases are hosted on are encrypted. Applications require specific menus/keys in VistA in order to access the information.

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

Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN are viewable in partial form.

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

Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN are viewable in partial form.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>Principle of Transparency:</u> 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?

DSS Enterprise (DSI) applications end users require a Veterans Health Information Systems and Technology Architecture (VistA)) *account and Active Directory network account; and VistA application-specific VistA menus and/or VistA security keys and may require role-based Active Directory security groups.*

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

DSS Enterprise (DSI) applications access is the responsibilities of the applications end users' local site OI&T personnel. Local site OI&T personnel follows their procedures and coordinate access with the applications end users' supervisor.

2.4c Does access require manager approval?

Yes DSS Enterprise (DSI) applications access is require manager/supervisor approval.

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

DSS Enterprise (DSI) applications interface with the Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker, Health Level 7 (HL7) or VistA Service Oriented Architecture (VSOA) technologies. DSS Enterprise (DSI) applications provide data input into the Veterans Health Information Systems and Technology Architecture (VistA) System files, as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU) and Clinical Patient Record System (CPRS) Problem List packages.

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

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS requests. New user's Veterans Health Information Systems and Technology Architecture (VistA) ePAS request can include VistA menu options/security keys, Clinical Patient Record System (CPRS) access, etc. There are application-specific VistA menu option/security keys, and VistA role-specific configuration.

All VHA staff are responsible for assuring safeguards for the PII.   Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly. VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current.

The system owner and managers are responsible for safeguarding PII/PHI

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 (Last name, First Name, Middle Initial)
Social Security Number
Date of Birth
Personal Mailing Address
Personal Phone Number(s)
Personal e-mail Address
Health Insurance Beneficiary Numbers Account Numbers
Current Medications
Previous Medical Records
Race/Ethnicity
Medical Record Number
Other Unique Identifying Number (ICN Internal Control Number)
Date of activity
Problem List
Attending Provider
Allergies
Laboratory Results
Surgeries
Admission Discharges and Transfers (ADTs)
Radiology Results
Vital Signs

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

DSS Enterprise (DSI) data is retained in accordance with the records disposition authority approved by the Archivist of the Unites States. The retention period for specific data will depend on which SORN that applies to that data. Here are the details for the SORNs this system uses:

SORN 79VA10, ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf states: Record Control Schedule (RCS) 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS 10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

SORN 24VA10A7, "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf states: "paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10-1, Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)."

SORN 121VA10, ''National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf indicates records are retained in accordance with General Records Schedule (GRS), 5.2, item 020 (https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf), that are described as intermediary records that are temporary and may be destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later.

RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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?

All records are within the system of records indicated with disposition authority approved by the Archivist of the Unites States.

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

As outlined in question 3.2 above record retention as it applies to data by SORN is as follows:

SORN 79VA10:
RCS 10–1, Item 2000.2, disposition authority DAA–GRS–2013–0005– 0004, item 020.
RCS 10–1, Item 2100.3, disposition authority DAA–GRS–2013–0006– 0004, item 31.

SORN 24VA10A7
RCS 10-1, Chapter 6, 6000.1d, disposition authority (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

SORN 121VA10,
GRS 5.2, Item 020, disposition authority DAA-GRS2022-0009-0001.
(https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf).

 RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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 data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin.

Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

DSS Enterprise patches (VistA KIDS build and GUI executable) are not released for National installation prior to testing. With an approved MOU (Memorandum of Understanding) from the IOC site(s), the vendor, Document Storage System (DSS), Test Patches are installed and tested in the VistA Pre-Production Test System. IOC site(s) tester(s) complete the Test Site(s) User's Acceptance VistA Pre-Production System document prior to VistA Production System installation. Test patients are created in the VistA Pre-Production Systems to be used when testing new DSS Enterprise (DSI) Patches. VistA Pre-Production Systems test patients' data are scrambled. Test shortcuts located on the application server

DocTest folder is mapped to the VistA Pre-Production System hostname and port number. Data is not provided from the DSI system for research purposes.

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: PII or PHI may be held for longer than it is required to be maintained. This extension of retention periods increases the risk that information may be breached or otherwise put at risk of access by unauthorized persons.

Mitigation: Of those applications that data is stored, the databases are encrypted, or the drive is encrypted. Access to these databases are restricted to only authorized users, administrative accounts. The standard user does not have access directly to the stored data.

To mitigate the risk posed by information retention, DSI adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual's information is carefully disposed of. The individual's information is carefully disposed of following the procedures listed in 3.4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Health Administration – VistA Imaging	Patient images are saved in the VistA Imaging System.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity	RPC (Remote Procedure Call) Broker
Veterans Health Administration – VistA/Vista VAEC AWS	Retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. summaries, lab, consult, imaging. The DSS Enterprise (DSI) is designed to provide diagnostic information, evaluate patient conditions, coding and	System Log files, sample clinical data that may contain Protected Health Information (PHI)	DSS Enterprise (DSI) uses RPC Broker, Health Level 7 (HL7), or VistA Service Oriented Architecture (VSOA) technologies which permit the

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
	crediting procedures, progress note (TIU (Text Integration Utilities)) are saved in VistA and images are saved in the VistA Imaging System. The use of the DSS Enterprise results in more accurate insurance billing for visits, consults and procedures. This application supports the filing of Encounters within the guidelines established by the Veterans Health Administration.)		application end users to retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System.
Veterans Health Administration – Clinicomp	User Login information is passed between ClinComp and VSOA in order to authenticate Clinicomp users.	User session log on information (Access Code/Verify Code)	HL7
Veterans Health Administration – Coding and Reimbursement System Plus	Retrieve and store clinical data within the Veterans Health Information and Technology Architecture (VistA) System. Coding & Reimbursement System Plus (CRS+) is designed to ensure coding accuracy supporting the coding, auditing, and billing functions using industry standard capabilities to ensure data accuracy for these purposes. Application provides users with support for selecting Evaluation & Management (E/M) codes, International Classification of Diseases 10 (ICD10) codes, Clinical Modification/Procedural Code Set (ICD10-CM/PCS) codes, Healthcare Common Procedure Coding System (HCPCS) codes and Common Procedure Terminology (CPT) codes. CRS+ interface with VistA Integration, Revenue, and Reporting (VIRR) s which interface with the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery.	Admission date, discharge date, age	RPC Broker

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII/PHI is that sharing data within the Department of Veteran's Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the population Healthcare and non-Healthcare providers. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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*
N/A				

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

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

Follow the format below:

<u>Privacy Risk:</u> T*here is no external sharing.*

<u>Mitigation:</u> *There is no external sharing.*

Section 6. Notice

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

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

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

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

The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. All enrolled Veterans and Veterans who are treated at VA Medical Centers but not required to enroll are provided the VHA Notice of Privacy Practices (NoPP) every three years, or sooner if a change necessitates an updated notice. The NoPP is also prominently posted in every VAMC (posters) and on the VA public-facing website. Link to VHA NoPP: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

Notice is also provided in the Federal Register with the publication of the following SORNs associated with this system:

> SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records–VA" https://www.govinfo.gov/content/pkg/FR-2020-12- 23/pdf/2020-28340.pdf.

> SORN 24VA10A7 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

> SORN 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

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

Notice was provided as indicated in question 6.1a above.

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.

Please see the response to 6.1a above for details.

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.

DSS Enterprise (DSI) extracts data that exists and was generated in the course of routine medical care. Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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 Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is provided. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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 that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NoPP when Veterans apply for benefits. Additionally, new NoPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to

provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NoPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at http://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

The system is not exempt from Privacy Act provisions.

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

The information in the system falls under Privacy Act systems of record and individuals have a right of access to request a copy of the information about themselves.

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

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

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NoPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call, or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

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

Mitigation: the risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The*/* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application users have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training. Staff roles are determined by the VistA Person Class codes. Providers must have a valid Person Class in VistA File 200 (New Person) File. Local VHA site OI&T is responsible to complete the ePAS request. OI& Technical staff complete the ePAS approval for System Administrator (grant server access), Application Administrator (manage application), and/or VistA Management (manage VistA System related tasks)

Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training.
Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers.

Note: Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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?

Other agencies do not have access to COTS Interface Division servers/applications.

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.

Each DSS Enterprise (DSI) application require application-specific VistA menu option(s) and/or VistA security key(s) to retrieve, create, and store data in VistA.

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 and vendors do not have access to COTS Interface Division servers/applications.

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 (for AITC technicians) 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 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. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 20-Apr-2023
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 08-Jun-2023
5. *The Authorization Termination Date:* 07-Jun-2025
6. *The Risk Review Completion Date:* 31-May-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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)*

System does not 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.*

System does not 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.

System does not 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.

System does not 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).

System does not use cloud technology.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

_____

Privacy Officer, Phillip Cauthers

_____

Information Systems Security Officer, Roland Parten

_____

Information Systems Owner, Gail Nemetz

APPENDIX A-6.1

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

VHA Handbook 1605.04, VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORNs:

Veterans Health Information Systems and Technology Architecture (VistA) Records - VA 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12- 23/pdf/2020-28340.pdf

Patient Medical Record – VA
24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10- 02/pdf/2020-21426.pdf

National Patient Databases – VA
121VA10A7 https://www.govinfo.gov/content/pkg/FR-2018-02- 12/pdf/2018-02760.pdf

HELPFUL LINKS:

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

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

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

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices