Date PIA submitted for review:

December 12, 2022

Privacy Impact Assessment for the VA Boundary called[1]:

Area Bath-Canandaigua
North Atlantic District 1

[1] The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, Boundary, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

Sites within Boundary:

Sites	***Station Numbers***
1) Bath VA Medical Center (VAMC)	528A6
2) Canandaigua VA Medical Center (VAMC)	528A5
3) Bath National Cemetery	803
4) Woodlawn National Cemetery	824
5) Rochester-Calkins VA Clinic	528QC
6) Elmira VA Clinic	528G4
7) Rochester-Clinton Crossings VA Clinic	528GE
8) Wellsville VA Clinic	528G8
9) Coudersport VA Clinic	528QE
10) Wellsboro VA Clinic	528QF
11) Rochester Vet Center	0124

Boundary Contacts:

Boundary Key Stakeholders

Name	***Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)***	***Phone Number***	***Email Address***	***Applicable Site (VBA, VHA, NCA, Program Office)***
Designated PO: Kathy Longwell	PO	(607) 664-4690	Kathy.Longwell@va.gov	VHA
Designated PO: Sherri Gamble	PO	(585) 393-7661	Sherri.Gamble2@va.gov	VHA
Designated PO: Cynthia Merritt	PO	(321) 200-7477	Cindy.Merritt@va.gov	NCA
Designated ISSO: Scott DeCaro	ISSO	(585) 393-7203	Scott.DeCaro@va.gov	VHA/NCA

Name	***Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)***	***Phone Number***	***Email Address***	***Applicable Site (VBA, VHA, NCA, Program Office)***
Designated ISSO: Ryan Gordon	ISSO	(585) 393-8580	Ryan.Gordon@va.gov	VHA/NCA
Designated ISO: Ali Meredith	AM	(607) 664-4843	Ali.Meredith@va.gov	VHA/NCA

Abstract

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

Area Bath-Canandaigua is an Information Boundary that consists of Bath VA Medical Center, Canandaigua VA Medical Center, Bath National Cemetery, Woodlawn National Cemetery, Rochester-Calkins VA Clinic, Elmira VA Clinic, Wellsville VA Clinic, Coudersport VA Clinic, Wellsboro VA Clinic, Rochester-Clinton Crossings VA Clinic and the Rochester Vet Center. The Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Boundary provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Boundary employs a myriad of routers and switches that connect to the VA network.

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:

- *The Boundary name and the name of the sites within it.*
- *The business purpose of the Boundary and how it relates to the program office and agency mission.*
- *Whether the Boundary is leveraging or accessing Enterprise repositories such as Veterans Benefits Management System, SharePoint, VistA, etc. and if so, a description of what PII/PHI from the Enterprise repositories is being used by the facilities in the Boundary.*
- *Documentation of any repository not maintained at the enterprise level, unlike Veterans Benefits Management System, SharePoint, VistA, etc. used by the facilities to collect, use, disseminate, maintain, or create PII/PHI.*
- *Any external information sharing conducted by the facilities within the Boundary.*
- *A citation of the legal authority to operate the Boundary.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *Does the Boundary host or maintain cloud technology? If so, does the Boundary have a FedRAMP provisional or agency authorization?*

The Area Bath-Canandaigua itself does not collect, use, disseminate, maintain, or store PII/PHI. VHA, VBA and NCA Facilities located within the Area Bath-Canandaigua IT Boundary all access VA Enterprise IT systems respectively, hosted and maintained outside of this boundary. These are VISTA, VBMS, MEM, etc.

Only PII/PHI collected and used by the facilities within the Boundary will be referenced in this document since the Boundary does not maintain, disseminate, or store information accessed by each facility. PII/PHI.

The facilities within the Boundary collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, VBMS, BOSS/AMASS, etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

The Boundary is using the VA Enterprise Cloud (VAEC) which is at the enterprise level and is outside of the Boundary. Further information can be found in the VAEC PIA.

The applicable SORs for Area Bath-Canandaigua include:

Applicable SORs

Site Type: VHA/NCA or Program Office	***Applicable System of Records (SORs)***
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10

Site Type: VHA/NCA or Program Office	*Applicable System of Records (SORs)*
	• Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10A7 • Health Information Exchange - VA 168VA005 • Applicants for Employment under Title 38, USC-VA, SORN 02VA135 • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending's, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN14VA05 • Police and Security Records – VA SOR 103VA07B • Accreditation Records – VA SOR 1VA022 • Blood Donor Information – VA SOR 04VA115 • Individual Correspondence Records – VA SOR 05VA026 • Employee Medical File System Records (Title 38) – VA SOR 08VA05 • Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations – VA SOR 09VA05 • Patient Advocate Tracking System Replacement (PATS–R) – VA SOR 100VA10H • Professional Standards Board Action and Proficiency Rating Folder (Title 38) – VA SOR 101VA05 • Agency-Initiated Personnel Actions (Title 38) – VA SOR 102VA05 • Police and Security Records – VA SOR 103VA07B • Agent Orange Registry – VA SOR 105VA10P4Q • Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations - VA SOR 106VA17 • Health Program Evaluation – VA SOR 107VA008B • Spinal Cord Injury and Disorders (SCI/D) Registry and Outcomes Program – VA SOR 108VA10NC9 • Employee Incentive Scholarship Program – VA SOR 110VA10 • Telephone Service for Clinical Care Records – VA SOR 113VA112 • Education Debt Reduction Program – VA SOR 115VA10 • Historical Alternative Dispute Resolution Data – VA SOR 116VA08 • Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce – VASOR 117VA10NA6 • Freedom of Information Act (FOIA) Records - VA SOR 119VA005R1C

Site Type: VHA/NCA or Program Office	*Applicable System of Records (SORs)*
	• Criminal Investigations – VA SOR 11VA51 • MyHealtheVet Administrative Records – VA SOR 130VA10P2 • Purchase Credit Card Program – VA SOR 131VA047 • Veterans Affairs/Department of Defense Identity Repository (VADIR) – VA SOR 138VA005Q • Individuals Submitting Invoices-Vouchers For Payment – VA SOR 13VA047 • Department of Veterans Affairs Federal Docket Management System Commenter Information (VAFDMS Commenter Info) – VA SOR 140VA00REG • Community Residential Care and Medical Foster Home Programs – VA SOR 142VA114 • General Counsel Legal Automation Workload System (GCLAWS) - VA SOR 144VA026 • Department of Veterans Affairs Personnel Security File System (VAPSFS) – VA SOR 145VA005Q3 • Department of Veterans Affairs Identity Management System (VAIDMS) – VA SOR 146VA005Q3 • Non-Health Data Analyses and Projections for VA Policy and Planning – VA SOR 149VA008A • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records – VA SOR 14VA135 • Administrative Data Repository – VA SOR 150VA19 • Inquiry Routing & Information System (IRIS) – VA SOR 151VA005OP6 • Ethics Web-based Database – VA SOR 152VA10 • Customer Relationship Management System (CRMS) – VA SOR 155VA10NB • Veterans Crisis Line Database – VA SOR 158VA10NC5 • All Employee Survey – VA SOR 160VA10A2 • Veterans Health Administration Human Capital Management – VA SOR 161VA10A2 • Investigative Database-OMI – VA SOR 162VA10E1B • Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT) – VA SOR 163VA005Q3 • Child Care Subsidy Program - VA SOR 165VA05CCSP • Veteran Child Care Programs – VA SOR 169VA10NC • Litigation Files – VA SOR 16VA026 • Principles of Excellence Centralized Complaint System – VA SOR 170VA22 • Human Resources Information Systems Shared Service Center (HRIS SSC) – VA SOR 171VA056A • VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP)-VA SOR 173VA005OP2

Site Type: VHA/NCA or Program Office	*Applicable System of Records (SORs)*
	• Loan Guaranty Fee Personnel and Program Participant Records – VA SOR 17VA26 • Centralized Staffing System – VA SOR 18VA05 • Motor Vehicle Operator Accident Records – VA SOR 20VA138 • Personnel and Accounting Integrated Data System – VA SOR 27VA047 • National Prosthetic Patient Database (NPPD) – VA SOR 33VA113 • Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance – VA SOR 36VA29 • Beneficiary Fiduciary Field System (BFFS) - VA SOR 37VA27 • Veterans Appellate Records System – VA SOR 44VA01 • Veterans Assistance Discharge System – VA SOR 45VA21 • Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA SOR 54VA10NB3 • Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records – VA SOR 55VA26 • Voluntary Service Records – VA SOR 57VA10B2A • Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA SOR 58VA21/22/28 • Repatriated Prisoners of War – VA SOR 60VA21 • Grievance Records – VA SOR 63VA05 • Readjustment Counseling Program (RCS) Vet Center Program – VA SOR 64VA10 • Inspector General Hotline (Complaint Center) Records VA SOR 66VA53 • VA Employee Counseling Services Program Records – VA SOR 68VA05 • Ionizing Radiation Registry – VA SOR 69VA10 • The Office of Inspector General Management Information System (MIS) – VA SOR 71VA53 • Health Professional Scholarship Program, and Visual Impairment and Orientation and Mobility Professional Scholarship Program – VA SOR 73VA10A2A • Department of Veteran's Affairs Secretary's Official Correspondence Records – VA SOR 75VA001B • General Personnel Records (Title 38) – VA SOR 76VA05 • VA Police Badge and Training Records System – VA SOR 83VA07 • Worker's Compensation-Occupational Safety and Health/Management Information System – VA SOR 86VA00S1 • Customer User Provisioning System (CUPS) – VA SOR 87VA005OP • Centralized Accounts Receivable System/Centralized Accounts Receivable On- Line System (CAR/CAROLS, combined system referred to as CAO) VA SOR 88VA244 • Call Detail Records – VA SOR 88VA244 • Gulf War Registry - VA SOR 93VA10

Site Type: VHA/NCA or Program Office	***Applicable System of Records (SORs)***
	• Consolidated Data Information System – VA SOR 97VA10 • Disaster Emergency Medical Personnel System (DEMPS) – VA SOR 98VA104
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records - VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records - VA SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records - VA, SOR 48VA40B • VA National Cemetery Pre-Need Eligibility Determination Records - VA SOR 175VA41A

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, Boundary, or technology being developed.

1.1 What information is collected, used, disseminated, or created, by the facilities within the Boundary?

Identify and list all PII/PHI that is collected and stored in the Boundary, including 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. If the Boundary creates information (for example, a score, analysis, or report), list the information the Boundary is responsible for creating.

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

Please check any information listed below that the facilities within the boundary collects. If additional PII/PHI is collected, 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 Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Next of Kin
☒ Guardian Information
☒ Electronic Protected Health Information (ePHI)

☒Military History/Service Connection
☒Service-connected Disabilities
☒Employment Information
☒ Veteran Dependent Information

- Service-connected rating
- Service Information
- Benefits Information
- Funeral Information
- Marital Status
- Relationship to Veteran

☒ Disclosure Requestor Information
☒ Death Certification Information
☒ Criminal Background
☒ Education Information
☒ Gender
☒ Tumor PHI Statistics

☐ Other Unique Identifying Information (list below)

PII Mapping of Components (Servers/Database)

Area Bath-Canandaigua consists of Seventeen key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within Area Bath-Canandaigua and the reasons for the collection of the PII are in the **Mapping of Components Table in Appendix B of this PIA.**

1.2 What are the sources of the information for the facilities within the Boundary?

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?

Describe why information from sources other than the individual is required. For example, if a facility program within the Boundary 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 1.3 indicate why the facility is using this source of data.
If a facility program within the Boundary creates information (for example, a score, analysis, or report), list the facility as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information that resides within the facilities in the Boundary is collected, maintained, and/or disseminated comes from a variety of sources. The largest amount of data comes directly from individuals - including veterans and their dependents, volunteers and other members of the public, clinical trainees, and VA employees and contractors. For example: items such as names, social security numbers, dates of birth are collected from the individual on healthcare enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares. An application for employment contains the same, or similar, information about employees.

Depending on the type of information, it may also come from Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers, Department of Defense (DOD), Internal Revenue Service (IRS), Office of Personnel Management (OPM), Social Security Administration (SSA), Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI).

Criminal background information is obtained from Electronic Questionnaires for Investigations Processing (E-QIP) and National Crime Information Center (NCIC) and used to confirm employment and/or volunteer eligibility and to assist the VA Police Service while conducting internal investigations.

1.3 How is the information collected?

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 Boundary, or created by the boundary itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Means of Collection Table

Site Type: VHA/NCA or Program Office	***Means of Collection***
VHA	Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or interviews and assessments with the individual. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.
NCA	MEM does receive information electronically from other systems, such as Veterans Benefits Management System (VBMS) eFolder via iHub, Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and User Provisioning,

Site Type: VHA/NCA or Program Office	*Means of Collection*
	VA Master Persons Index Enterprise (MPIe), and direct conversation with individual Veterans or Next of Kin. Information is received, reviewed, and collected through inbound and outbound telephone engagement, in-person contact, postal mail, and fax, to the National Cemetery Scheduling Office (NCSO), Applicant Assistance Unit (AAU), national cemeteries, and other NCA offices. Data is manually entered into all NCA systems except for the Enterprise Eligibility Office Automation System (EOAS). EOAS receives applications and documents via direct upload from VA.gov. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD-214, are scanned/uploaded into the document repositories such as FEITH, EOAS, and eFolder and stored in the Memorial Data Warehouse. AMAS processes approximately 360,000 claims for standard government headstones or markers (VA Form 40-1330) and Monument and Presidential Memorial Certificate Request (VA Form 40-0247) applications annually. Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.

Information related to an employee's employment application may be gathered from the applicant for employment, which is provided to an application processing website, USA Jobs.

Information from outside resources comes to the Area Bath-Canandaigua using several methods, to include site to site connection, facsimile and/or email. Chief among these sources, are the DoD, SSA, and IRS. The DoD provides military records, including medical records compiled when the patient was a member of the US Military. Income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

These data collections may be done using secure web portals, VPN connection, e-mail, and facsimile.

NCA: The Memorial Benefits Management System (MBMS) is under development to replace the BOSS-E and AMAS system suite. MBMS has replaced BOSS-E as the primary scheduling tool at the NCSO and will replace all NCA systems to include BOSS, AMAS, EOAS, Web-Presidential Memorial Certificates (Web-PMC), and Memorial Enterprise Letters (MEL) by 2025.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular PII/PHI is collected, maintained, used, or disseminated in the Boundary is necessary to the program's or agency's mission. Merely stating the general purpose of the Boundary without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the Boundary collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the Boundary's purpose. This question is related to privacy control AP-2, Purpose Specification.

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by Area Bath-Canandaigua are as varied as the types of information collected.

Much of the information collected is maintained, used, and disseminated to ensure that Veterans and other eligible individuals obtain the medical and mental health treatment they require. Additional information, such as bank account information and insurance information are used to process claims and requests for benefits. Other purposes include determination of legal authority for providers and other clinical staff to practice medicine and/or subject matter expertise, release of information request responses, and research/analysis of data.

Purpose of Information Collection Table

Site Type: VHA/NCA or Program Office	***Purpose of Information Collection***
VHA	• To determine eligibility for health care and continuity of care • Emergency contact information is cases of emergency situations such as medical emergencies • Provide medical care • Communication with Veterans/patients and their families/emergency contacts • Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise • Responding to release of information request • Third party health care plan billing, e.g. private insurance • Statistical analysis of patient treatment • Contact for employment eligibility/verification
NCA	• MEM collects and maintains information to verify the identity and eligibility of the Veteran, decedent, beneficiary, and personal representative/funeral home for burial and monument benefits and monument services

1.5 How will the information collected and used by the facilities be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in a facility within the Boundary is checked for accuracy. Is information within the facility 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 a facility within the Boundaries that receives data from internal data sources or VA IT systems, describe the checks to ensure that data corruption has not occurred during transmission.

If the Boundary checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information that is collected and used directly from enterprise systems have additional details regarding checks for accuracy in their own enterprise level PIAs.

Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered an individual’s medical record by a doctor or other medical staff is also assumed to be accurate and is not verified.

Information is checked through the VBA to verify eligibility for VA benefits. Information about military service history is verified against official DoD military records and income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

Employee, contractor, student, and volunteer information is obtained by automated tools as well as obtained directly by the individuals. The Federal Bureau of Investigation and Office of Personnel Management are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources.

For NCA, Standard operating procedures (SOPs) are in place at NCA offices and cemeteries to perform quality control on data related to each case. As cases progress through the queues from NCSO case managers to the cemetery office staff, additional data integrity checks are conducted. Final data integrity checks are performed by cemetery operations staff who perform the interment after services.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the Boundary, 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

Legal Authority Table

Site Type: VHA/NCA or Program Office	**Legal Authority**
VHA	• Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program.
NCA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(a), 501(b), and Chapter 24, Sections 2400-2404. • 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 • 5 U.S.C. § 552a, Privacy Act of 1974, As Amended • 48VA40B – Veterans (Deceased) Headstone or Marker Records-VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404. • Public Law 100---503, Computer Matching and Privacy Act of 1988 • Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397 • OMB Circular A---130, Management of Federal Information Resources, 1996 • OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites • OMB Memo M---99---18, Privacy Policies on Federal Web Sites • OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions • OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII • The Health Insurance Portability and Accountability Act of 1996 (HIPAA) • State Privacy Laws

	• The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:
VA Area Bath-Canandaigua collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:
VA Area Bath-Canandaigua employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The boundary employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

All employees with access to Veteran's health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.

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 within the Boundary will be used in support of the program's business purpose.

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

- **Name**: Used to identify the patient during appointments and in other forms of communication
- **Social Security Number**: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
- **Date of Birth**: Used to identify age and confirm patient identity
- **Mother's Maiden Name:** Used to confirm patient identity
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- **Email Address**: used for communication and MyHealtheVet secure communications
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual):** Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third part Health care plans
- **Certificate/License numbers**: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.

- **Vehicle License Plate Number**: Used for assignment of employee parking and assignment of parking during events
- **Internet Protocol (IP) Address Numbers**: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- **Current Medications**: Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
- **Previous Medical Records**: Used for continuity of health care
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Tax Identification Number**: Used for employment, eligibility verification
- **Medical Record Number**: Used to identify a patient within the medical record system without using their social security number as their identifier.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.
- **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information**: Used to track and account for patient medical records released to requestors.
- **Death certificate information**: Used to determine date, location and cause of death.
- **Criminal background information**: Used to determine employment eligibility and during VA Police investigations.
- **Education Information**: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
- **Gender**: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan
- **Death certificate information**: Used to determine date, location and cause of death.
- **Date of Death:** Used to verify spousal and beneficiary relationship to Veteran, at time of death

- **Marital Status:** Used to verify spousal and beneficiary eligibility
- **Service Information:** Used to verify eligibility
- **Benefit Information:** Used to verify burial benefits
- **Relationship to Veteran:** Used to determine relationship to Veteran
- **Funeral Home Information:** Used to contact funeral home or other service coordinator information

The data may be used for approved research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; the registration of vehicles and the assignment and utilization of parking spaces; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the facility 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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The VA Area Bath-Canandaigua uses statistics and analysis to create general reports that provide the VA a better understanding of patient care and needs. These reports are:

1. Reports created to analyze statistical analysis on case mixes.
2. Analyze the number of places and geographical locations where patients are seen to assess the volume of clinical need.
3. Analyze appointment time-frame data to track and trend averages of time.

These reports may track:

- The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc. for Veterans established with a Patient Care Aligned Team (PACT)
- Beneficiary travel summary/benefits
- Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII/PHI determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII/PHI being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII/PHI?

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

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?

<u>Principle of Use Limitation:</u> Is the use of information contained in the facilities 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.

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal administrative rounds during which personal examine all areas within the facility to ensure information is being appropriately used and controlled.

Data such as patient wait times, provider case load, and VA employee time and attendance is used to perform daily operational tracking and trending.

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 by the facilities within the Boundary?

Identify and list all information collected from question 1.1 that is retained by the facilities within the Boundary.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The Area Bath-Canandaigua itself, does not retain information.

- Name
- Previous medical records
- Social Security Number (SSN)
- Race/ethnicity
- Date of Birth
- Next of Kin
- Mother's Maiden Name
- Guardian Information
- Mailing Address
- ePHI
- Zip Code
- Military history/service connection
- Phone Numbers
- Service connection disabilities
- Fax Numbers
- Employment information
- Email address
- Veteran dependent information
- Emergency contact info
- Disclosure requestor information
- Financial account information
- Death certification information
- Health insurance beneficiary account numbers
- Tumor PII/PHI statistics
- Certificate/license numbers

- Criminal background investigation
- Internet Protocol address numbers
- Education Information
- Current medications
- Gender
- Tax Identification Number
- Medical Record Number
- Vehicle License Plate Numbers
- Service Information
- Benefit Information
- Relationship to Veteran
- Funeral Home Information
- Name and address of Next of Kin

Military service data, applicant's name and address, place of burial, burial service and headstone data.

3.2 How long is information retained by the facilities?

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 Boundary may have a different retention period than medical records or education records held within your Boundary, 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.

This question is related to privacy control DM-2, Data Retention and Disposal.

Length of Retention Table

Site Type: VHA/NCA or Program Office	***Length of Retention***
VHA	• Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS)10-1, Part Two, Chapter Four- Finance Management • Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d. • Official Human Resources Personnel File: Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1

	- Office of Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1.
NCA	- Veterans (Deceased) Headstone or Marker Records-VA SORN 48VA40B: Retained indefinitely

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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 Boundary owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

Retention Schedule Table

Site Type: VBA/VHA/NCA or Program Office	***Retention Schedule***
VHA	Records Control Schedule 10-1 Records Control Schedule 005-1
NCA	Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B. NCA RCS

3.4 What are the procedures for the elimination of PII/PHI?

Explain how records are destroyed or eliminated at the end of the 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

Information within the Area Bath-Canandaigua is destroyed by the disposition guidance of *RCS 10-1*. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

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 the **Department of Veterans' Affairs Directive 6500 VA Cybersecurity Program (January 23, 2019)**. 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 per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

3.5 Does the Boundary include any facility or program that, where feasible, uses 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

No PII is used to test systems prior to deployment. All testing is conducted with test samples of the required application categorization of the subject.

For NCA, PII collected by Memorial (MEM) is not used for research, testing or training.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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 Boundary.

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

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> There is a risk that the information maintained by Area Bath-Canandaigua could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, Area Bath-Canandaigua adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The Area Bath-Canandaigua ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, use and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the boundary to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

NCA: File plans are created by each individual office/facility, according to NCA RCS and GRS. File plans are updated and inventoried annually or as needed for business.

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 are facilities within the Boundary sharing/receiving/transmitting information with? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Note: Question #3.5 (second table) in the Boundary 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 Boundary 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 each facility, 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 internally by facilities within the Boundary including VA Enterprise Systems 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 data element types such as PII/PHI that are shared/received with the Program Office or IT System***	***Describe the method of transmittal***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Veterans Benefits Administration (VBMS)	Filing benefit claims	Financial assessment test and service-connected disability diagnoses, veterans' health status, compensation and pension exam notes	Compensation and Pension Record Interchange (CAPRI) electronic software package	Bath VAMC (VHA) Canandaigua VAMC (VHA)
Veterans Health Administration (VistA)	Electronic Health Record	System Log files, sample clinical data that may contain patient name, SSN, diagnosis, Date of Birth, medications, appointments, health insurance and next of kin.	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	Bath VAMC (VHA) Canandaigua VAMC (VHA)
National Cemetery Administration	Memorial Benefits Management System (MBMS); BOSS (Burial Operations Support System); AMAS (Automated Monument Application System); MADSS (Management and Decision Support System); EOAS (Eligibility Office	Benefits, decedent, claimant, requestor, and beneficiary information (such as names, addresses, social security numbers)	Information may be transmitted upon request in a written or verbal format based on the individual request; Electronically shared via network connections	Bath National Cemetery (NCA) Woodlawn National Cemetery (NCA)

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 data element types such as PII/PHI that are shared/received with the Program Office or IT System***	***Describe the method of transmittal***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
	Automation System); PMCS (Presidential Memorial Certificate System) Veterans Benefit Management System (VBMS); Master Person Index (MPI)			
Identity and Access Management (IAM)	User access control	PII - Identity Access Information for User access control: Name, Address, SSN (Data Encrypted)	REST Web Service API (HTTP)	NCA- National cemeteries and other NCA offices, as needed for processing
Burial Operations Support System - Enterprise (BOSS-E)	To support legacy users	Memorial Information; Birth Date, Email, Name, Gender, Address, Date of Death, Marital Status, Military honors, Relationship to Veteran, SSN, Phone, County, Military Service Release from Active Duty (RAD) Date, Veteran's Period of Service, and Veteran's War Period	Secure Database Connection - Oracle Forms based application backed by an Oracle 12c database	NCA- National cemeteries and other NCA offices, as needed for processing
VA Master Persons Index (MPI)-Enterprise (MPIe)	To have the ability to search the authoritative data source for Veterans, MPI, to ensure that they are not creating duplicate contact records in applications built	First Name, Middle Name, Last Name, Social Security Number (SSN), Date of Birth (DOB), Gender, Phone Number, Place of Birth (POB) City, Place of Birth (POB) State, Mother's Maiden Name	REST Web Service API (HTTP)	NCA- National cemeteries and other NCA offices, as needed for processing

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 data element types such as PII/PHI that are shared/received with the Program Office or IT System***	***Describe the method of transmittal***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
	on the Salesforce platform.			
VA Tumor Register	Tumor Register	Diagnosis & procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, hormone, radiation, chemotherapy, problem lists	Electronic tumor register package	Bath VAMC (VHA) Canandaigua VAMC (VHA)
VA HIV Register	HIV Register	Diagnosis & procedures, HIV/AIDS status, treatment outcome, survivor tracking, type of treatments, demographics, problem lists	Electronic HIV catalogue package	Bath VAMC (VHA) Canandaigua VAMC (VHA)
VA Network Authorization office - NON-VA Care Payments	Fee Basis Claim System (FBCS)	Demographics, diagnoses, medical history, service connection, Provider orders, VHA recommendation/approval for non-VA care	Fee Basis Claim System (FBCS) authorization software program	Bath VAMC (VHA) Canandaigua VAMC (VHA)
Consolidated Patient Account Center	CPAC	Diagnosis, service connection, dates of service, health insurance information, demographics	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	Bath VAMC (VHA) Canandaigua VAMC (VHA)
VA Health Eligibility Center	HEC	Service dates, SSAN, demographics, service connection	Scanned documents uploaded into shared software program	Bath VAMC (VHA) Canandaigua VAMC (VHA)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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.

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

Follow the format below:

<u>Privacy Risk:</u> The internal sharing of data is necessary individuals to receive benefits at the Area Bath-Canandaigua. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

<u>Mitigation:</u> Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a “least privilege/need to know” policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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 facility is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: Question #3.6 in the Boundary 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 Boundary 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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
New York State Department of Health	Patient Care and State Regulatory Requirements	Health information regarding infectious disease and PII/PHI to include patient's name, lab results, and contact information	Title 10 New York Codes Rules and Regulations (10NYCRR); Title 38, United States Code, Section 5701; SORN 24VA10A7	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
IRS - Internal Revenue Services	Income verification	Information is shared as the IRS requires the use of identifying data, including names and SSNs, in order for VA to request and receive data	SORN 89VA10NB Income Verification Records-VA; Privacy Act of 1974, 5 United States	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
			Code 552a(e), Public Law 101-508 Omnibus Budget Reconciliation Act of 1990		
DoD - Department of Defense	Determine military service dates, eligibility	Name, SSN, Information contained in the medical record Provider Notes Nursing Notes	MOU; Privacy Act of 1974, 5 United States Code 552a; Public Law 104-191; Title 38, United States Code, Sections 320, 5106, 5701, 7332	Joint Legacy Viewer (JLV); CPRS; secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Social Security Administration	Patient Care	Social Security Number, Protected Health Information (PHI) contained in the medical record. Provider Notes Nursing Notes Operative Reports Medication Lists Radiology Test Reports Laboratory Test Reports	Title 38, United States Code, Section 5701; SORN 79VA10	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
New York State Office of Children and Family Services (OCFS) –	Patient Care and State Regulatory Requirements	Health information regarding suspicion of, and case of, child abuse and neglect; PII/PHI to	New York State Social Services Law Sections 413-415, 422 and	via secure fax and secure portal	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Statewide Central Register of Child Abuse and Maltreatment (SCR)		include patient's name, lab results, and contact information	424;	verbal disclosures via telephone	Canandaigua VA Medical Center (VHA)
New York State Office of Children and Family Services (OCFS) – Protective Services for Adults	Patient Care and State Regulatory Requirements	Health information regarding infectious disease, PII/PHI to include patient's name, lab results, and contact information	New York State Social Services Law § 473; New York Codes Rules and Regulations (18NYCRR Part 457); Title 38, United States Code, Section 5701; VHA Standing Request Letter	via secure fax and verbal disclosures via telephone	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
New York State Department of Health – Bureau of Vital Records	Patient Care and State Regulatory Requirements	Health information regarding infectious disease, PII/PHI to include patient's name, lab results, and contact information	Title 10 New York Codes Rules and Regulations (10NYCRR); Title 38, United States Code, Section 5701; SORN 24VA10A7	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Center for Disease Control (CDC)		Provision of health care reporting to include Name, SSN, Information contained in the medical record	Standing Letter Request	via secure fax and secure web portal	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		Provider Notes Nursing Notes			Canandaigua VA Medical Center (VHA)
Centers for Medicare and Medicaid Services (CMS)		Provision of health care reporting to include Name, SSN, Information contained in the medical record Provider Notes Nursing Notes	SORN 97VA10 Consolidated Data Information System-VA; Title 38, United States Code Section 527; Public Law 103-62	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Food and Drug Administration (FDA)		Veteran/patient PII/PHI to include names, SSN, DOB, diagnosis, provider information and medication	Federal Food, Drug, and Cosmetic Act; written authorization; subpoena, or court order	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Office of Human Research Protections (OHRP)		Veteran/patient PII/PHI to include names, SSN, DOB, diagnosis, provider information and medication.	MOU; Facility Institutional Review Board (IRB); VHA Handbooks 1100.19 and 1200.05; Title 38, United States Code Sections 501, 7331, 7334	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Department of Health and Human Services. (DHHS)		Health information regarding infectious disease, PII/PHI to include patient's name, lab results, and contact information	Privacy Act of 1974, 5 United States Code 552a; Public Law 104-191; Title 38, United States Code, Sections 5701, 5705, 7332	via secure fax and secure web portal	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Abbott Rapid Diagnostics (Formerly Alere)	System Support	No PII, PHI, or VA Sensitive Information is transmitted.	National ISA/MOU	Remote Access VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
GE Healthcare (GEHC)	Patient care and System Support	Service-specific data to perform remote support, limited data sets with specific PHI elements depending on application such as patient name, DOB, record ID, images, waveforms, and gender will be transmitted from the GE Healthcare Systems on the VA network to GE	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		Healthcare OnLine Center.			
OPM Fingerprint Transaction System (FTS)	Initial Background Investigation	Fingerprints and PII information are sent to OPM as part of the initial background screening and PIV Card issuance.	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Phillips HealthTech	Patient care and System Support	System Performance Parameters / System Monitoring information, which may include but are not limited to disk usage, reconstruction speed, image quality parameters, Helium levels, temperature, humidity. • System Error Code Information • Acquisition Parameter Settings / System maintenance information such as scan time, kV, mA, XRay	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		tube heat • Patient Images for image artifact troubleshooting (may also include patient demographic data / Personal Identity information)			
Parata Systems LLC	System Support	Parata Systems does not normally receive, process, or store customer Protected Health Information (PHI). In the rare events when PHI is received by Parata for troubleshooting purposes, it is safeguarded in accordance with industry best practices including but not limited to the controls described in the subsequent sections.	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
ScriptPro LLC/ScriptPro USA	Patient Care and System Support	System Log files, drug database updates, software updates, patient identifiers such as SSN, DOB and de-	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		identified information			Canandaigua VA Medical Center (VHA)
Sysmex America	System Support	System Log files and software updates	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Siemens Healthcare Diagnostics/Siemens Medical Solutions	Patient Care and System Support	System Log files, sample clinical data that may contain patient name, test results, medical record number, patient identifier, and accession number	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
UTECH	System Support	System Log files and software updates. No sensitive information is transmitted.	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Vecna Technologies, Inc.	System Support	System Log files and software updates and patches. No sensitive information is transmitted.	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
AFGA Healthcare Corporation	Patient Care and System Support	Log files and sample clinical data from VA sites which may contain HIPAA Protected Health Information (PHI). Last name, Date of Birth (DOB), Social Security Number (SSN), Sex and Patient Address	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Vocera Communications, Inc	Patient Care and System Support	Personal Identifiable Information (PII) and electronic Protected Health Information (ePHI) collected may include name, DOB, gender, Medical Information, clinical images, biometrics and Other ID Number	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Barco, Inc.		There is NO transmission of VA sensitive data. The data transmitted is the luminance response data for the diagnostic displays and pertains to the	National ISA/MOU	All data will be communicated over port 443 using HTTPS using a secure VPN interconnection between VA and Barco	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		displays DICOM Greyscale Display Function (GSDF) compliance, also included in the data transmission is the display's serial number and other internal display characteristic information			
Becton Dickinson (Formerly CareFusion, LLC (Pyxis, Alaris)	System Support	System Log files and software updates	National ISA/MOU	SSL/TLS tunnel over port 443 using the Remote Support Service (RSS) Software	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
McKesson Corporation	System Support	No VA owned sensitive data. Data includes online ordering, inventory management and scanning management information.	National ISA/MOU	Firewall Waiver	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
LabCorp-Quest Diagnostics, Inc.	Patient Care	The data types are stored, collected or disseminated with LEDI: • Patient Name • DOB • Sex • Patient ID	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
		• Order or accession number • VA facility code • Client or account number • Order code(s) and names • Any comments associated with the orders • Any specimen source or type required, as applicable			
Canon Medical Systems USA, Inc (Formally Toshiba America Medical Systems)	Patient Care and System Support	Secure file transfer, automatic collection of system health information, system log analysis tools, automatic notification for system alerts, Image Quality Assurance (QA) analysis, and other various diagnostic and DICOM utility applications. No Personally Identifiable Information (PII), Protected Health Information (PHI),	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		or VA Sensitive Information is transmitted			
Stored Value Solutions (SVS)	Veteran Canteen Service Sales and Payment	The transmitted data contains anonymous numbers that are not associated with any Personal Identification Information (PII), and Protected Health Information (PHI). The transmitted bar-coded Universal Product Code (UPC) information of the activation approval or declined, balance of the sale transaction from the POS through the Acceo Tender Retail Merchant Connect Multi software to SVS Gift Card System	National ISA/MOU	TLS encryption and supports the Payment Card Industry Security Standard (PCI SSC) as required	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Roche Diagnostics	Patient Care and System Support	Select log files containing system telemetry and (potentially) Protected Health Information (PHI) (limited to specific,	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		VA controlled data elements specifying medical test orders and results), would be transferred from the VA's Roche devices to the Roche Customer Support Center. This information can contain test identifier (ID), sample ID, patient ID, and quality metrics. Each system is configurable to allow for reduced usage of patient PHI. (Tests can be run using only sample ID).			Canandaigua VA Medical Center (VHA)
The Department of the Treasury Bureau of the Fiscal Service Worldpay, LLC, LLC	Veteran Canteen Service Sales and Payment	The data collected will include: Financial Account Information, Name, Social Security Number, Personal Phone, and Personal Email.	National ISA/MOU	All communications between the POS and server will be secured with HTTPS. The encryption will use TLS v1.2.	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Rotronic Instrument Corp.	Temperature Monitoring Services	Transmits temperature data from local devices.	Local ISA/MOU	All communication will be	Canandaigua VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		No VA owned sensitive data is transmitted.		outbound traffic via HTTPS 443	
Hill-Rom Company Inc	System Support	The transmission includes network data could include, but is not limited to, a variety of software applications for services and technical log files. Also, remote desktop support, remote software deployment, and remote monitoring capabilities, as well as technical data and log files for troubleshooting	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA)
Cepheid	To expedite the processing of data associated with VA and Cepheid.	Incidental access to ePHI may occur during remote support sessions. ePHI on the GeneXpert family of systems consists of Patient ID, Patient Name, and Sample ID. test archive files are de-identified by the lab user using functionality within	National ISA/MOU	SSL/TLS tunnel over port 443	Bath VA Medical Center (VHA)

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		the GeneXpert software			
Abbott Laboratories	System Support	The Abbott Instrumentation transmits Abbott instrument logs and related files for maintenance reports, test counts by assay, calibration logs and diagnostic message history. Each Abbott instrument has its own unique identifier. The transmitted data doesn't contain PII, PHI, or any VA sensitive information.	National ISA/MOU	Site to Site (S2S) VPN Tunnel	Bath VA Medical Center (VHA) Canandaigua VA Medical Center (VHA)
Box.Com Cloud (VA)	Secure File transfers with Business Partners	Information includes DOB, SSN, VA Patient Genomic Information, Age, Gender, Race as well as non-VA Sensitive data	System Level ISA/MOU	Information will be transmitted to Box Inc. Systems over SSL port 443.	Canandaigua VAMC (VHA)
BOSS and Veterans Benefits Management Service (VBMS) – State and	Benefits, decedent, claimant, requestor, and beneficiary	Names, addresses, service information, marriage/dependent status,	MOU in Draft	Electronic access within the system	State and Tribal cemeteries located within the area

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 data element types such as PII/PHI that are shared/received 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***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Tribal cemeteries	information	and social security numbers)			
Salesforce	The MBMS application will need to push/pull data from existing NCA data sources via Rest APIs exposed by MBMS. Functionality build includes Case Management, Eligibility, and Scheduling	Names, addresses, service information, marriage /dependent status, and social security numbers	48VA40B – Veterans (Deceased) Headstone or Marker Records-VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404. ISA/MOU between Salesforce and MBMS system	Service Based	State and Tribal cemeteries located within the area
VAEC AWS	AWS hosted in VAEC is the government cloud that will serve as the infrastructure that hosts the BIP platform as a service and subsequent hosted minor application, MBMS.	Names, addresses, service information, marriage /dependent status, and social security numbers	MBMS is a minor application under the BIP Platform ATO – all VAEC AWS agreements are between BIP and VAEC	Hosted Environment	State and Tribal cemeteries located within the area

The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

Internal protection is managed by access controls such as user authentication (user IDs, passwords and Personal Identification Verification (PIV)), awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the *Area Bath-Canandaigua*. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.

All personnel accessing Veteran’s information must first have a successfully adjudicated background screening or Special Agreement Check (SAC). This background check is conducted by the Office of Personnel Management A background investigation is required commensurate with the individual's duties.

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 in Appendix A. (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?

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. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the facilities within the Boundary 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.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, Boundary of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Area Bath-Canandaigua. provides notice of information collection in several additional ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA System of Record Notices (VA SORN) in the Federal Register and online.

Applicable SORs

Site Type: VHA/NCA or Program Office	*Applicable SORs*
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10A4

Site Type: VHA/NCA or Program Office	***Applicable SORs***
	• Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005 • Applicants for Employment under Title 38, USC-VA, SORN 02VA135 • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending's, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN14VA135 • Police and Security Records – VA SOR 103VA07B • Accreditation Records – VA SOR 01VA022 • Blood Donor Information – VA SOR 04VA115 • Individual Correspondence Records – VA SOR 05VA026 • Employee Medical File System Records (Title 38) – VA SOR 08VA05 • Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations – VA SOR 09VA05 • Patient Advocate Tracking System Replacement (PATS–R) – VA SOR 100VA10H • Professional Standards Board Action and Proficiency Rating Folder (Title 38) – VA SOR 101VA05 • Agency-Initiated Personnel Actions (Title 38) – VA SOR 102VA05 • Agent Orange Registry – VA SOR 105VA10P4Q • Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA SOR 106VA17 • Health Program Evaluation – VA SOR 107VA008B • Spinal Cord Injury and Disorders (SCI/D) Registry and Outcomes Program – VA SOR 108VA10NC9 • Employee Incentive Scholarship Program – VA SOR 110VA10 • Telephone Service for Clinical Care Records – VA SOR 113VA112 • Education Debt Reduction Program – VA SOR 115VA10 • Historical Alternative Dispute Resolution Data – VA SOR 116VA08 • Veterans Canteen Service (VCS) Payroll Deduction Program (PDP), Point of Sale (POS) Help Desk and eCommerce – VASOR 117VA10NA6 • Freedom of Information Act (FOIA) Records - VA SOR 119VA005R1C • Criminal Investigations – VA SOR 11VA51 • MyHealtheVet Administrative Records – VA SOR 130VA10P2 • Purchase Credit Card Program – VA SOR 131VA047

Site Type: VHA/NCA or Program Office	*Applicable SORs*
	• Veterans Affairs/Department of Defense Identity Repository (VADIR) – VA SOR 138VA005Q • Individuals Submitting Invoices-Vouchers For Payment – VA SOR 13VA047 • Department of Veterans Affairs Federal Docket Management System Commenter Information (VAFDMS Commenter Info) – VA SOR 140VA00REG • Community Residential Care and Medical Foster Home Programs – VA SOR 142VA114 • General Counsel Legal Automation Workload System (GCLAWS) - VA SOR 144VA026 • Department of Veterans Affairs Personnel Security File System (VAPSFS) – VA SOR 145VA005Q3 • Department of Veterans Affairs Identity Management System (VAIDMS) – VA SOR 146VA005Q3 • Non-Health Data Analyses and Projections for VA Policy and Planning – VA SOR 149VA008A • Administrative Data Repository – VA SOR 150VA19 • Inquiry Routing & Information System (IRIS) – VA SOR 151VA005OP6 • Ethics Web-based Database – VA SOR 152VA10 • Customer Relationship Management System (CRMS) – VA SOR 155VA10NB • Veterans Crisis Line Database – VA SOR 158VA10NC5 • All Employee Survey – VA SOR 160VA10A2 • Veterans' Health Administration Human Capital Management – VA SOR 161VA10A2 • Investigative Database-OMI – VA SOR 162VA10E1B • Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT) – VA SOR 163VA005Q3 • Child Care Subsidy Program - VA SOR 165VA05CCSP • Veteran Child Care Programs – VA SOR 169VA10NC • Litigation Files – VA SOR 16VA026 • Principles of Excellence Centralized Complaint System – VA SOR 170VA22 • Human Resources Information Systems Shared Service Center (HRIS SSC) – VA SOR 171VA056A • VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP)-VA SOR 173VA005OP2 • Loan Guaranty Fee Personnel and Program Participant Records – VA SOR 17VA26 • Centralized Staffing System – VA SOR 18VA05 • Motor Vehicle Operator Accident Records – VA SOR 20VA138 • Personnel and Accounting Integrated Data System – VA SOR 27VA047 • National Prosthetic Patient Database (NPPD) – VA SOR 33VA113

Site Type: VHA/NCA or Program Office	*Applicable SORs*
	• Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance – VA SOR 36VA29 • Beneficiary Fiduciary Field System (BFFS) - VA SOR 37VA27 • Veterans Appellate Records System – VA SOR 44VA01 • Veterans Assistance Discharge System – VA SOR 45VA21 • Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA SOR 54VA10NB3 • Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records – VA SOR 55VA26 • Voluntary Service Records – VA SOR 57VA10B2A • Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA SOR 58VA21/22/28 • Repatriated Prisoners of War – VA SOR 60VA21 • Grievance Records – VA SOR 63VA05 • Readjustment Counseling Program (RCS) Vet Center Program – VA SOR 64VA10 • Inspector General Hotline (Complaint Center) Records VA SOR 66VA53 • VA Employee Counseling Services Program Records – VA SOR 68VA05 • Ionizing Radiation Registry – VA SOR 69VA10 • The Office of Inspector General Management Information System (MIS) – VA SOR 71VA53 • Health Professional Scholarship Program, and Visual Impairment and Orientation and Mobility Professional Scholarship Program – VA SOR 73VA10A2A • Department of Veteran's Affairs Secretary's Official Correspondence Records – VA SOR 75VA001B • General Personnel Records (Title 38) – VA SOR 76VA05 • VA Police Badge and Training Records System – VA SOR 83VA07 • Worker's Compensation-Occupational Safety and Health/Management Information System – VA SOR 86VA00S1 • Customer User Provisioning System (CUPS) – VA SOR 87VA005OP • Centralized Accounts Receivable System/Centralized Accounts Receivable On- Line System (CAR/CAROLS, combined system referred to as CAO) VA SOR 88VA244 • Call Detail Records – VA SOR 90VA194 • Gulf War Registry - VA SOR 93VA10 • Consolidated Data Information System – VA SOR 97VA10 • Disaster Emergency Medical Personnel System (DEMPS) – VA SOR 98VA104
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41

Site Type: VHA/NCA or Program Office	***Applicable SORs***
	• Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B • VA National Cemetery Pre-Need Eligibility Determination Records -VA SOR 175VA41A

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

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis.

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

The Area Bath-Canandaigua only requests information 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.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Area Bath-Canandaigua.

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

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

This question is related to privacy control IP-1, Consent

Information Consent Rights Table

Site Type: VBA VHA, NCA or Program Office	***Information Consent Rights***
VHA	Yes. Individuals must submit in writing to their facility PO. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out. Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. Individuals have the right to consent to particular uses of information by completing the VA Form 10-5345 (Request for and Authorization to Release Health Information) that can be used for third party release or VA Form 10-5345a (Individuals' Request for A Copy of Their Own Health Information).
NCA	Responding to collection is voluntary; therefore, consent of use is not applicable.

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.

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 veterans and other members of the public will not know that the Area Bath-Canandaigua exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.
Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. s. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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?

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 to obtain information about FOIA points of contact and information about agency FOIA processes.

If the facilities within the Boundary are 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).

If the facilities within the Boundary are not a Privacy Act Boundary, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the "office concerned," the request may be addressed to the PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: *Individuals' Request for a Copy of their Own Health Information*, which can be obtained from the medical center or online at https://www.va.gov/find-forms/about-form-10-5345a/.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the myHeal*the*Vet program, VA's online personal health record. More information about my Heal*the*Vet is available at https://www.myhealth.va.gov/index.html.

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).

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>

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, a veteran or other VAMC patient who is enrolled in myHealthevet can use the system to make direct edits to their health records.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this Boundary 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.

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> 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: Area Bath-Canandaigua mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records.

The Area Bath-Canandaigua 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 Boundary, and are they documented?

Describe the process by which an individual receives access to the Boundary.

Identify users from other agencies who may have access to the Boundary and under what roles these individuals have access to the Boundary. Who establishes the criteria for what PII can be shared?

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

This question is related to privacy control AR-7, Privacy-Enhanced Boundary Design and Development.

Individuals receive access to the Area Bath-Canandaigua by gainful employment in the VA or upon being awarded a contract that requires access to the boundary systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. VA Area Bath-Canandaigua requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

Access is requested utilizing Electronic Permission Access Boundary (ePAS) and YourIT User Provisioning. Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA Area Bath-Canandaigua is generally limited by appropriate locking devices and restricted to authorized VA IT employees. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.

Access to the Area Bath-Canandaigua working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee’s functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Human Resources will notify Divisions, IT and ISSO of new hires and their start date(s), through via email. Local IT will get notifications as well via YourIT User Provisioning and EPAS requests. Supervisor and/or designee, as well as Contracting Officers Representatives (CORs), will submit an EPAS request to gain local IT approval for access. VISN HR, as well as CORs, will submit YourIT User Provisioning requests that will get routed to local IT for approval.

- Individuals are subject to a background investigation before given access to Veteran’s information.

• All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually AND Privacy and HIPAA Focused Training.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the Boundary 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 will have access to the Boundary after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Boundary only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA Area Bath-Canandaigua access must have an approved computer access request on file. The area manager, or designee, in conjunction with the ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules.

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

VA offers privacy and security training. Each program or Boundary may offer training specific to the program or Boundary that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

All Area Bath-Canandaigua personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the Boundary Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses:

VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics.
VA 31167: Privacy and Information Security Awareness and Rules of Behavior-Print
VA 3847875: Training Reciprocity-Annual Privacy and Information Training
VHA 3185966: VHA Mandatory Training for Trainees
VHA 3192008: VHA Mandatory Training for Trainees-Refresher
VA 10203: Privacy and HIPPA Training
VA 10204: Privacy and HIPPA Training-Print
VA 20152: Mandatory Training for Transient Clinical Staff

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

8.4a If Yes, provide:

1. *The Systems Security Plan Status:* ***Complete***
2. *The Systems Security Plan Status Date:* ***September 1, 2022***
3. *The Authorization Status:* ***Authorization to Operate (ATO)***
4. *The Authorization Date:* ***May 20, 2022***
5. *The Authorization Termination Date:* ***May 19, 2025***
6. *The Risk Review Completion Date:* ***September 1, 2022***
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* ***MODERATE***

Please note that all Boundaries containing PII/PHI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

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

Section 9. 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 Boundary 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	Boundary of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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

Signature of Privacy Officers

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

KATHY LONGWELL Digitally signed by KATHY LONGWELL
Date: 2022.12.29 08:01:15 -05'00'

Privacy Officer, Kathy Longwell

Sherri L Gamble 235965 Digitally signed by Sherri L Gamble 235965
Date: 2022.12.29 08:11:19 -05'00'

Privacy Officer, Sherri Gamble

Cynthia A. Merritt 297052 Digitally signed by Cynthia A. Merritt 297052
Date: 2022.12.28 15:50:40 -05'00'

Privacy Officer, Cynthia Merritt

Signature of Information System Security Officers

The Information System Security Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Scott A DeCaro 614270 Digitally signed by Scott A DeCaro 614270
Date: 2022.12.29 06:53:50 -05'00'

Information System Security Officer, Scott DeCaro

RYAN GORDON Digitally signed by RYAN GORDON
Date: 2022.12.29 07:31:48 -05'00'

Information System Security Officer, Ryan Gordon

Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

ALI MEREDITH Digitally signed by ALI MEREDITH
Date: 2023.01.06 15:28:46 -05'00'

Area Manager, Ali Meredith

APPENDIX A – Notice

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).

Applicable Notices

Site Type: VBA/VHA/NCA or Program Office	***Applicable NOPPs***
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
NCA	**VA Form 40-0247** **VA Form 40-1330** **VA Form 40-1330M**

APPENDIX B – PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapping of Components (Servers/Database)

Components of the Boundary collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Bath SQL 1: • EFORMS • LICENSE • SOLUTIONINFO • WEBAPPCONFIG	Yes	Yes	No	Patient/Next of Kin and Employee Sensitive Data to include name, DOB, diagnosis, SSN# and contact information.	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Bath VA Medical Center
Canandaigua SQL 1: • EFORMS • LICENSE • SOLUTIONINFO • WEBAPPCONFIG	Yes	Yes	No	Patient/Next of Kin and Employee Sensitive Data to include name, DOB,	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	Canandaigua VA Medical Center

Components of the Boundary collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
				diagnosis, SSN# and contact information.		managed with restricted access controls	
Canandaigua SQL 19: • Censis_Beta_V2_Global • censis_graphics • Censis_HL1598 • Censis_SG1598 • CensisBufferAgent	Yes	Yes	No	Patient/Next of Kin and Employee Sensitive Data to include name, DOB, diagnosis, SSN# and contact information.	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Canandaigua VA Medical Center

APPENDIX C – List of Medical Devices and Special Purpose Systems

Name of Device	Type (Medical Device or Special Purpose System)	Is the device within the MedMOD boundary?	Enterprise Risk Assessment Number
n/a			