Date PIA submitted for review:
06/15/2021

Privacy Impact Assessment for the VA Area Boundary called1:

Area Erie
North Atlantic District

Facilities Supported by the Area

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Erie VA Medical Center</td>
</tr>
<tr>
<td>2</td>
<td>Ashtabula County Community Based Outpatient Clinic</td>
</tr>
<tr>
<td>3</td>
<td>Crawford County Community Based Outpatient Clinic</td>
</tr>
<tr>
<td>4</td>
<td>McKean County Community Based Outpatient Clinic</td>
</tr>
<tr>
<td>5</td>
<td>Venango County Community Based Outpatient Clinic</td>
</tr>
</tbody>
</table>

---

1 The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, Area 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.
6. Warren County Community Based Outpatient Clinic

7. Erie Vet Center

8. Lanza Administrative Annex

**Area Boundary Contacts:**

**Area Privacy Officer**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone Number</th>
<th>Email Address</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated Area PO:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richard Arthur</td>
<td>814 860-2523</td>
<td><a href="mailto:Richard.arthur@va.gov">Richard.arthur@va.gov</a></td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Richard Doray</td>
<td>814 860-2922</td>
<td><a href="mailto:Richard.doray@va.gov">Richard.doray@va.gov</a></td>
<td>Erie VAMC</td>
</tr>
</tbody>
</table>

**Area Information System Security Officer**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone Number</th>
<th>Email Address</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated Area ISSO:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paul Mascatelli</td>
<td>814 860-2636</td>
<td><a href="mailto:Paul.mascatelli@va.gov">Paul.mascatelli@va.gov</a></td>
<td>Paul Mascatelli</td>
</tr>
</tbody>
</table>

**Area Manager**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone Number</th>
<th>Email Address</th>
<th>Location</th>
</tr>
</thead>
</table>
Abstract

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

Erie Area is an Information Systems Boundary that consists of Erie VA Medical Center, Ashtabula County Community Based Outpatient Clinic (CBOC), Crawford County CBOC, McKean County CBOC, Venango County CBOC, Warren County CBOC, Erie Vet Center, and the Lanza Administrative Annex. The Area 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 Area 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 Area 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 Area 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 Area 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 IT Area Boundary name and the name of the sites within it.
- The business purpose of the Area Boundary and how it relates to the program office and agency mission.
- Whether the Area 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 PII/PHI from the Enterprise repositories is being used by the facilities in the Area 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/PII/PHI.
- Any external information sharing conducted by the facilities within the Area Boundary.
- A citation of the legal authority to operate the Area 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 Area Boundary host or maintain cloud technology? If so, Does the Area Boundary have a FedRAMP provisional or agency authorization?

Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?

NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the Cloud Service Provider or its customers (VA) be affected?

The Area 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 systems environment also includes as applicable, subsystem components such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances and tier 2 storage solutions. The systems 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 Information Systems employ a myriad of routers and switches that connect to the VA network.

This information system is continuously used during business and non-business hours, supporting many businesses processing within the agency’s computing environment and a single repository for the Veterans’ electronic health records. The confidentiality, integrity and availability of the Area Erie System is critical, i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of this information system, all personnel with system administration rights and roles will required an elevated background investigation to fulfill their duties. The boundary for this assessment and authorization is intended to review and assess the management, operational, and technical security controls associated with all IT hardware, including servers, printers, scanners, and all other peripheral devices desktop computer systems and all operating systems software currently operating under the management control of Area Erie.

The Area Erie itself does not collect, use, disseminate, maintain, or store PII/PHI.

VHA, VBA and NCA Facilities located within the Erie Area 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 Area will be referenced in this document since the Area IT boundary does not maintain, disseminate or store information accessed by each facility. PII/PHI.

The legal authorities include Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974.

The completion of this PIA will not result in any business or technology changes for the area.
The facilities within the Area IT 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 applicable SORs for Area Erie include:

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Applicable SORs</th>
</tr>
</thead>
</table>
| VHA                                    | • Non-VA Fee Basis Records-VA, SOR 23VA10NB3  
• Patient Medical Records-VA, SOR 24VA10P2  
• Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA12  
• 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 79VA10P2  
• 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 114VA10D  
• National Patient Databases-VA, SOR 121VA10A7  
• Enrollment and Eligibility Records- VA 147VA10NF1  
• VHA Corporate Data Warehouse- VA 172VA10P2  
• Applicants for Employment under Title 38, USC-VA, SORN 24VA10P2, 79VA10P2  
• Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05135 (Nov. 18, 2010)  
• Non-VA Fee Basis Records-VA, SORN 23VA163 (Aug. 31, 2014) |

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, Area Boundary, or technology being developed.

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

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

If a requesting Area Boundary receives information from another Area Boundary, such as a response to a background check, describe what information is returned to the requesting Area 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 area 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
- Other Unique Identifying Number (list below)

Next of kin, guardian information, electronic protected health information (ePHI), military history/service connection/non-service connected status, service connected disabilities, employment information, Veteran dependent information, disclosure requestor information, death certificate information, tumor PII (personal identifiable information) and PHI (protected health information) statistics, criminal background information, education information, gender.

Area Erie consists of three key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Area Erie and the functions that collect it are mapped below. Each component has been analyzed to determine if any elements of that component collect PII.

**PII Mapping of Components**

The type of PII collected within Area Erie 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 Area 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 Area 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 Area 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 collected, maintained, and/or disseminated by the Area Boundary is derived from various sources. The information may come directly from the Veteran or other programs and resources in the Veterans Benefits Administration (VBA), VA Health Eligibility Center (HEC), Department of Defense (DOD), VA Network Authorization Office (NAO) for non-VA care payments, and non-VA providers. Criminal background information is obtained from National Crime Information Center (NCIC) and used to confirm employment and/or volunteer eligibility and to assist the VA Police Service with conducting internal investigations.

The information that resides within the facilities in the Area 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.

Additional sources include:
- VA, Compensation, Pension, Education and Rehabilitation Records
- VA, Veterans and Beneficiaries Identification Records Location Subsystem
- VA, 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records
• VA, 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records
• VA, Veterans and Beneficiaries Identification and Records Location (BIRLS)
• Compensation, Pension, Education and Rehabilitation (covers BDN and Corporate databases)
• Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records
• VA, 53VA00 Veterans Mortgage Life Insurance

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 Area Boundary, or created by the area 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

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Means of Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>VHA</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 Erie using several methods. Usually from electronic transfer of information. 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
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 Area Boundary is necessary to the program’s or agency’s mission. Merely stating the general purpose of the Area Boundary without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

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

Information is collected, maintained, and processed by Area Erie for the following purposes:

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by Area Erie 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**

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Purpose of Information Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>VHA</td>
<td>• To determine eligibility for health care and continuity of care</td>
</tr>
<tr>
<td></td>
<td>• Emergency contact information is cases of emergency situations such as medical emergencies</td>
</tr>
<tr>
<td></td>
<td>• Provide medical care</td>
</tr>
<tr>
<td></td>
<td>• Communication with Veterans/patients and their families/emergency contacts</td>
</tr>
<tr>
<td></td>
<td>• Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise</td>
</tr>
<tr>
<td></td>
<td>• Responding to release of information request</td>
</tr>
<tr>
<td></td>
<td>• Third party health care plan billing, e.g. private insurance</td>
</tr>
<tr>
<td></td>
<td>• Statistical analysis of patient treatment</td>
</tr>
<tr>
<td></td>
<td>• Contact for employment eligibility/verification</td>
</tr>
</tbody>
</table>

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 Area 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 Area 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 Area 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.

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.

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

List the full legal authority for operating the Area 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

The legal authorities that defined the collection of information include the Veterans Benefits Act, Chapter 73: Veterans Health Administration – Organization and Functions, Title 38, U.S.C. § 7301.


Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009

Legal Authority Table

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Legal Authority</th>
</tr>
</thead>
</table>
| 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 §§300jj et seq.; §§17901 et seq.)  
• VHA Directive 1605.01 Privacy & Release of Information  

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:
Area Erie 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:
Area Erie 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 area 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 HSPD12. 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 Area 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 My HealtheVet 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.

• **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.

• **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
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 Area 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 Area 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

Area Erie utilizes statistics and analysis to create various reports, which provide a better understanding of patient care and needs. These reports are:
- The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc.
  for Veterans enrolled into a Patient Care Aligned Team
- 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

**PRIVACY IMPACT ASSESSMENT: Use of the information.** 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. *Example:* Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or Area Boundary controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

**Principle of Use Limitation:** Is the use of information contained in the 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.

Each employee is assigned a functional category that determines the level of access to PII and PHI. The functional category is assigned by the supervisor. Computer menu options are approved by the Supervisor and Information Security Officer based on the functional category assigned and the need to know for the employee to perform their job duties. All staff is responsible for safeguarding PII and PHI. Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA’s stated purpose for using the data.

These controls include mandatory training for all employees, volunteers, and contractors; monitoring inappropriate access through security logs; review of staff menu and security keys; monitoring functional categories for minimum access, etc.

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

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

The Area Erie Boundary 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

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 Area Boundary may have a different retention period than medical records or education records held within your Area 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**

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Length of Retention</th>
</tr>
</thead>
</table>
| 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. |

**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 Area Boundary owner.

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

**Retention Schedule Table**

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Retention Schedule</th>
</tr>
</thead>
</table>
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 Erie is destroyed by the disposition guidance of RCS 10-1, VB-1, maintained for 75 years. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014).

Additionally, the Area Erie follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization, and Erie VAMC Area Media Protection SOP, July 13, 2020.

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.

Paper records are shredded on-site by a shredding company, witnessed by the Records Management Officer, and are accompanied by a certificate of destruction. Non-paper records maintained on magnetic media are destroyed by erasing the magnetic media using an approved software to digitally overwrite the media. The media is then shredded on-site by the contracted shredding company, witnessed by the Records Management Officer per VBA Directive 6300.

3.5 Does the Area 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
Area Erie does not conduct research therefore, the Area Boundary does not store research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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 Area Boundary.

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

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

*Principle of Data Quality and Integrity:* Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

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

*Privacy Risk:* There is a risk that the information maintained by Area Erie 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 Area Erie adheres to the VA RCS 10-1 Schedules for each category of data it maintains. When the data retention is reached, Area Erie will dispose of the information per the mechanism described in question 3.4.

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 6 on Privacy Threshold Analysis should be used to answer this question.

**4.1 With which internal organizations are facilities within the Area Boundary sharing/receiving/transmitting information with? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT Area 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 Area including VA Enterprise Systems Organizations

<table>
<thead>
<tr>
<th>Internal Organization Name</th>
<th>IT System Name</th>
<th>Data Elements</th>
<th>Method of Transmission</th>
<th>Applicable Area Site (VBA, VHA, NCA, Program Office)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Network Authorization Office-Non-VA Care Payments</td>
<td>VA Network Authorization Officer</td>
<td>Demographics, diagnoses, medical history, service connection, Provider orders, VHA recommendation - approval for non-VA care</td>
<td>Fee Basis Claim System (FBCS) authorization software program</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>VA Tumor Registry</td>
<td>VHA</td>
<td>System Log files, sample clinical data that may contain Protected Health Information (PHI)</td>
<td>Electronically pulled from VistA thru Computerized Patient Record System (CPRS)</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Program Office</td>
<td>IT Area Boundary</td>
<td>Data Element Types</td>
<td>Method of Transmittal</td>
<td>Applicable Area Sites</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Veterans Benefits Administration VBA</td>
<td>Financial assessment test and service-connected disability diagnoses, veterans’ health status, compensation and pension exam notes</td>
<td>Compensation and Pension Record Interchange (CAPRI) electronic software package</td>
<td>Erie VAMC</td>
<td></td>
</tr>
<tr>
<td>Veterans Administration HEC</td>
<td>Diagnosis, service connection, dates of service, health insurance information, demographics</td>
<td>Enrollment Systems Redesign or automatic upload to health Eligibility Center (HEC) via a Veterans Information Systems and Technology Architecture (Vista)</td>
<td>Erie VAMC</td>
<td></td>
</tr>
<tr>
<td>VA National Cemetery Administration</td>
<td>VA National Cemetery Administration</td>
<td>Veteran’s name, social security number, branch of service, military discharge papers – Form DD214</td>
<td>Secure fax</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>NECPAC</td>
<td>Diagnosis, service connection, dates of service, health insurance information, demographics</td>
<td>Veterans Information Systems and Technology Architecture (VISTA)</td>
<td>Erie VAMC</td>
<td></td>
</tr>
</tbody>
</table>

Version Date: September 3, 2020
Page 21 of 45
<table>
<thead>
<tr>
<th>Consolidated Mail Outpatient Pharmacy (CMOP)</th>
<th>CMOP</th>
<th>Veteran’s name, address, full social security number, date of birth, provider’s name, name/quantity of medication(s), provide name</th>
<th>Veterans Information Systems and Technology Architecture (VISTA)</th>
<th>Erie VAMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Personnel Management (OPM)</td>
<td>OPM</td>
<td>Employee name, demographics, date of birth, social security number, employment files</td>
<td>Uploaded to Office of Personnel Management</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>VBMS</td>
<td>Filing benefit claims</td>
<td>Social Security Number, Benefits Information, Claims Decision, DD-214</td>
<td>Compensation and Pension Record Interchange (CAPRI) electronic software package</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>VistA</td>
<td>Electronic Health Record</td>
<td>Area Boundary Log files, sample clinical data that may contain Protected Health Information (PHI)</td>
<td>Electronically pulled from VistA thru Computerized Patient Record Area Boundary (CPRS)</td>
<td>Erie VAMC</td>
</tr>
</tbody>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

**Privacy Risk:** The internal sharing of data is necessary individuals to receive benefits at the Area Erie. 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.

**Mitigation:** 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: This question is #7 in the Privacy Threshold Analysis.**

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 an Area 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**

<table>
<thead>
<tr>
<th>System Name and External Organization or Agency Name</th>
<th>Data Elements Shared/Received</th>
<th>Type of Connection</th>
<th>Agreement Type (Can be more than one)</th>
<th>Applicable Area Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center for Organ Recovery (CORE)</td>
<td>PII/PHI</td>
<td>Via secure fax and/or notification by phone call</td>
<td>45 § 164.512(g)-(i)</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>System Name and External Organization or Agency Name</td>
<td>Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
<td>Applicable Area Site</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Pennsylvania Department of Health Infectious Disease</td>
<td>PHI, PII, and Individually Identifiable Information (III) appropriate to the state law.</td>
<td>Secure fax, Telephone, PA – National Electronic Disease Surveillance System (PA-NEDSS)</td>
<td>24VA10P2 RU# 4 Standing Request Letter</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Pennsylvania Department of Health – Cancer Registry</td>
<td>PHI, PII, and III appropriate to the state law.</td>
<td>Secured transmission through Web Plus (internet-based application developed by the Centers for Disease Control and Prevention, National Program of Cancer Registries)</td>
<td>Data Use Agreement (DUA)</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Pennsylvania Department of Aging</td>
<td>PII</td>
<td>Via phone call to Department of Aging</td>
<td>Standing Request Letter</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Centers for Medicare and Medicaid Services (CMS)</td>
<td>PII, PHI</td>
<td>Secure transmissions, SFTP &amp; VPN</td>
<td>Sharing Agreement</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>System Name and External Organization Name</td>
<td>Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
<td>Applicable Area Site</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>-------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Social Security Administration</td>
<td>Veteran's primary contact, social security number, date of birth, race, addresses, military, medical, criminal record, guardian, education, financial, health insurance, benefit and claims information. (Title 38, United States Code, Section 5701)</td>
<td>Site to Site (S2S), IPSEC Tunnel, Secure FTP</td>
<td>National Interconnection Security an Erie VAMC Agreement (ISA), Memorandum of Understanding (MOU)</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>IRS - Internal Revenue Services</td>
<td>Veteran's primary contact, SSN, date of birth, race, addresses, military, medical, criminal record, guardian, education, financial, health insurance, benefit and claims information</td>
<td>Secure Web-Portal, Secure Socket Layer</td>
<td>National MOU/ISA, Computer Matching Agreement</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>DoD - Department of Defense</td>
<td>PII, PHI</td>
<td>Bi-directional Health Information Exchange</td>
<td>MOU</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Federal Bureau of Investigation (FBI)</td>
<td>Employee name</td>
<td>In person, encrypted email, electronic via FBI website</td>
<td>24VA10P2 RU# 4 VA SORN 02VA135; VA SORN 79VA19</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>System Name and External Organization Name</td>
<td>Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
<td>Applicable Area Site</td>
</tr>
<tr>
<td>Veteran Service Organizations (VSO)</td>
<td>Veteran's primary contact, SSN, date of birth, race, addresses, medical, criminal record, guardian, education, financial, health insurance, benefit and claims information.</td>
<td>Secure transmissions, SFTP &amp; VPN</td>
<td>Patient written authorization for read only access to Computerized Patient Record System (CPRS)</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Pennsylvania State Prescription Drug Monitoring Program (SPDMP)</td>
<td>PII</td>
<td>Query through the centralized State Prescription Drug Monitoring Program</td>
<td>24VA10P2</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Phillips Healthcare</td>
<td>Demographic data, PII, patient images for image artifact troubleshooting</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Topcon Medical Systems</td>
<td>PHI</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Alere Informatics Inc.</td>
<td>PHI</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>ScriptPro USA, Inc.</td>
<td>Prescription data that may include PHI and PII during the course of troubleshooting and maintenance support</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Vecna Technologies, Inc.</td>
<td>Demographics, PII</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>GetWellNetwork, Inc.</td>
<td>PII, PHI</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>System Name and External Organization or Agency Name</td>
<td>Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
<td>Applicable Area Site</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Quest Diagnostics, Inc.</td>
<td>Patient Name, DOB, Sex, Patient ID, 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.</td>
<td>Health Level 7 (HL7) messaging; courier service for delivering specimens</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Roche Diagnostics</td>
<td>Clinical chemistry and immunoassay test information transmitted and received can contain test ID, sample ID, patient ID, and quality metrics.</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>PICIS Clinical Solutions, Inc.</td>
<td>PHI during the course of troubleshooting and maintenance support</td>
<td>VPN</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>National Crime Information Center (NCIC)</td>
<td>PHI, PII, III</td>
<td>Secure transmission through Personal Management Fingerprint Transaction System (FTS)</td>
<td>National MOU/ISA</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>Fee-Based Providers</td>
<td>PHI, PII</td>
<td>Secured transmissions through VPN access or via secure fax</td>
<td>Signed VA Privacy and Information Security Rules of Behavior</td>
<td>Erie VAMC</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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.

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the Area Erie. 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 Area 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, Area Boundary of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Area Erie 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. Additional notice is provided through the Notice of Privacy Practices (NOPP) and Privacy Impact Assessments (PIA) which is available online as required by the eGovernment Act of 2002, Pub.L.107-347 § 208(b)(1)(B)(iii) 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.
### Site Type: VBA/VHA/NCA or Program Office

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Applicable SORs</th>
</tr>
</thead>
</table>
| VHA                                    | • Non-VA Fee Basis Records-VA, SOR 23VA10NB3  
  • Patient Medical Records-VA, SOR 24VA10P21  
  • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA12  
  • Community Placement Program-VA, SOR 65VA122 |

### Site Type: VBA/VHA/NCA or Program Office

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Applicable SORs</th>
</tr>
</thead>
</table>
|                                         | • Health Care Provider Credentialing and Privileging Records-VA, SOR 77VA10E2E  
  • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10P2  
  • Income Verification Records-VA, SOR 89VA10NB  
  • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131  
  • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D  
  • National Patient Databases-VA, SOR 121VA10A7  
  • Enrollment and Eligibility Records- VA 147-VA10NF1  
  • VHA Corporate Data Warehouse- VA 172VA10P2 |

This Privacy Impact Assessment (PIA) also serves as notice of the Area Erie. 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.

The following Written notice is on all VA forms: PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching.

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 Erie 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. Individuals have the opportunity to decline to provide information without a penalty with the exception of the means test process. Non-service-connected Veterans and Veterans who are in receipt of service-connected compensation of less than 50% may decline to give a financial assessment called a means test and as a result, may be placed in category 8 and billed for certain services.

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

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

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Information Consent Rights</th>
</tr>
</thead>
</table>

Version Date: September 3, 2020
Page 31 of 45
Yes. Individuals must submit the 10-5345 (Request for Authorization to Release Medical Records or Health Information) to state with whom his/her information may be shared. In writing to their facility Release of Information Office. 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 optout, 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.

<table>
<thead>
<tr>
<th>6.4 PRIVACY IMPACT ASSESSMENT: Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.</td>
</tr>
</tbody>
</table>

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:

**Privacy Risk:** There is a risk that veterans and other members of the public will not know that the Area Erie 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 (N OPP) 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 Area 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 Area Boundary are not a Privacy Act Area 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.

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 http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf

Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the My HealtheVet program which is VA’s online personal health record. More information regarding My HealtheVet may be found at https://www.myhealth.va.gov/index.html

As directed in VA SOR Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28(July 19, 2012), individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. A list of regional VA offices may be found on the VBA Website.

In addition to the procedures discussed above, the SORNs listed in question 6.1 address record access, redress, and correction. Links to all VA SORNs may be found at http://www.oprm.va.gov/privacy/systems_of_records.aspx

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 http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the my HealthVet program, VA’s online personal health record. More information about my HealthVet 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 provided the opportunity to submit a request for change in a medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual may request an alteration to their health information by making a formal, written request mailed or delivered to the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A request for amendment of information contained in a system of records will be processed by the Privacy Officer (PO). In reviewing requests to amend or correct records, the PO must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility Business Office for processing.

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.

Verbal inquiries regarding the amendment request process are generally received by the Release of Information Office, Patient Experience Officer, or Privacy Officer. Inquiries regarding the amendment request process can be explained by any member of the Release of Information Office, Patient Experience Officer or the Privacy Officer. The amendment process is also explained in the Notice of Privacy Practices (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 area 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. Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The Privacy Officer provides procedures for appeal rights to the Office of General Counsel or VHA Privacy Office via the written response to the Veteran regarding the outcome of the amendment request, per NOPP.

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 my HealtheVet can use the system to make direct edits to their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this Area 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:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Privacy Risk: There is a risk that Veterans, whose records contain erroneous information, may not receive notification of appointments, medications, or test results. Incorrect documentation could also result in a Veteran receiving improper diagnosis or treatment.

Mitigation: The Area Erie boundary mitigates the risk of incorrect information in an individual’s records by authenticating information when possible using the resources discussed in question 1.5. The Erie VAMC staff verifies information in medical records and corrects information identified as incorrect during each patient’s medical appointment. Veterans have the right to request and amendment of health information when it is believed that the information is incomplete, inaccurate, untimely, or unrelated to their health care. The Notice of Privacy Practices (NOPP) discusses this amendment process.

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

The Area Erie 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 My-HealtheVet 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 Area Boundary, and are they documented?

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

Identify users from other agencies who may have access to the Area Boundary and under what roles these individuals have access to the Area 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 Area 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 Area Boundary Design and Development.

Individuals receive role-based access to the Area Boundary through employment in the VA, upon being awarded a contract that requires access to the Area systems, or upon completion of an education agreement. Upon acceptance of employment, a request for a user account is submitted by Human Resources, Contract Officer Representatives (COR), or the Education department, using the ServiceNow/YourIT (YourIT) web interface. Based on the submitted requests, the National Service Desk (NSD) creates the accounts, which are reviewed and modified by local Office of Information and Technology (OI&T) account managers. Once finalized, the new accounts are accessed by the employee/contractor/student using two-factor authentication (2FA), unless exempted for technical reasons (such as software incompatibility with 2FA technologies or positional restrictions). Exemption from 2FA is reviewed and approved by the user’s supervisor/COR.

For changes to existing accounts, service chiefs/service line managers (for access modifications, e.g. employment terminations, change in position) or Human Resources (for changes to user identification, e.g. legal name changes) will notify OI&T of the change, within 24 hours, by submitting a request through the YourIT web interface.

Access is requested using the Electronic Permission Access System (ePAS). New user requests are submitted by Human Resources, Contract Officer Representatives (COR), or the Education department, based on need to know and/or job duties. Requests are submitted for VA employees, contractors, students, and all outside agency requests, and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system using 2FA or with a username/password combination, which follow authentication complexity guidelines.

Human Resources notifies divisions and OI&T of new hires and their start date(s), either through email and/or YourIT. The division receiving the employee/contractor/student submits requests via YourIT and ePAS for role-based access. Depending on the system access requested, requests may contain the user’s name, SSN and/or claim number, job title, division, telephone number,
required training dates, along with access the user will need on the computer system. At a minimum the requests start at the division level, is signed by the supervisor and Area Manager, and then goes to the appropriate account management team for action.

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.

Role based training is required for individuals with significant information security responsibilities to include, but not limited to, the Information System Security Officer (ISSO), the Area Manager, System Administrators, Network Administrators, Database Managers, users of VA Information Systems or VA Sensitive Information.

Access to information stored on electronic storage media at other VA locations is controlled by individually unique passwords/codes.

The YourIT and ePAS web interfaces follow processes and workflows to ensure they are compliant with VA Handbook 6500/Knowledge Service requirements and the National Institute of Standards and Technology (NIST) controls. Account requests, at a minimum, require approval of the employee’s supervisor and the Area Manager.

Strict physical security control measures are implemented to further protect areas containing sensitive information and materials. Access to restricted spaces is based on an employee’s functional category as well as the completion of role-specific training. VA file areas are locked after normal duty hours. Access to information technology sensitive areas at VA Erie is limited by appropriate locking devices and restricted to authorized VA OI&T employees. The facilities are protected from outside access by the Federal Protective Service or other security personnel.

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.

Veteran Service Representatives (VSR) and Rating Veteran Service Representatives (RVSR) have access to amend/change the information in the system, under the guidelines of least privilege. Veteran Service Organizations (Co-located VSOs) and County or Out based VSOs (CVSOs) also have access to VA systems. These accesses are predefined and limited for these users. Individuals are subject to a background investigation before given access to Veteran’s information. Private Attorneys, Claim Agents and Veteran Service Organizations Representatives must be accredited through the Office of General Counsel.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the Area 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.

Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area Boundary only after completing mandatory information security and privacy training, 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 Area Erie access must have an approved computer access request on file. The area manager, or designee, in conjunction with the area 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 Area Boundary?

VA offers privacy and security training. Each program or Area Boundary may offer training specific to the program or Area 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 Erie 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 training by the area 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.

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and

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

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

Area Erie is currently under a nine-month Authority to Operate (ATO) granted on 3 December 2020. The systems under VA Erie are classified as a MODERATE risk per FIPS 199. Area Erie is due for a review on 3 September 2021.

Section 9. References

Summary of Privacy Controls by Family

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

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

RICHARD G. ARTHUR 1672842

Privacy Officer

Signature of Information Security Systems Officers

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

Paul D Mascatelli 209531

Information Security Systems Officer

Signature of Area Manager

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

Gregory L. Forinash 750326

Area Manager
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

<table>
<thead>
<tr>
<th>Site Type: VBA/VHA/NCA or Program Office</th>
<th>Applicable NOPPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>VHA</td>
<td>Notice of Privacy Practices</td>
</tr>
<tr>
<td></td>
<td>VHA Privacy and Release of Information:</td>
</tr>
<tr>
<td>^VBA</td>
<td>Privacy Statement on VA Forms:</td>
</tr>
</tbody>
</table>

**PRIVACY ACT INFORMATION:** The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefit for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

**SOR 58VA21/22/28**
APPENDIX B – PII Mapped to Components

The completion of this section of the PIA will be in coordination with the Area Manager, Privacy Officer and ISSO. They may need to coordinate with the system (server/database) point of contact.

**PII Mapped to Components Table**

<table>
<thead>
<tr>
<th>Components of the Area Boundary collecting/storing PII (Each row refers to a grouping of databases associated with a single server)</th>
<th>Does this component collect PII? (Yes/No)</th>
<th>Does this component store PII? (Yes/No)</th>
<th>Does this component share, receive, and/or transmit PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
<th>Provide Names of Applicable Sites</th>
</tr>
</thead>
</table>
| **Server 1:**  
  • Candidate Mailing Output Database  
  • Genesis Utility Database  
  • Recruitment Enrollment App | Yes | Yes | Yes | Social Security Number, EKG reading, Blood Pressure | 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 |  |
| **Server 2:**  
  • Candidate Stage Database | Yes | Yes | Yes | Social Security Number, Name, Address | To provide and manage benefits for the veteran | Advanced Encryption Standard (AES) 256, Server is stored in a secured environment |  |
<table>
<thead>
<tr>
<th>Components of the Area Boundary collecting/storing PII (Each row refers to a grouping of databases associated with a single server)</th>
<th>Does this component collect PII? (Yes/No)</th>
<th>Does this component store PII? (Yes/No)</th>
<th>Does this component share, receive, and/or transmit PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
<th>Provide Names of Applicable Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>managed with restricted access controls</td>
</tr>
</tbody>
</table>