Privacy Impact Assessment for the VA IT System called:

Area Fargo
Midwest District Territory 1

Date PIA submitted for review:

8/19/2020

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer, VHA</td>
<td>Rhonda Cross</td>
<td><a href="mailto:Rhonda.cross@va.gov">Rhonda.cross@va.gov</a></td>
<td>701-239-3700 ext. 3978</td>
</tr>
<tr>
<td>Privacy Officer, VBA</td>
<td>Cheryl Asmund</td>
<td><a href="mailto:Cheryl.Asmund@va.gov">Cheryl.Asmund@va.gov</a></td>
<td>701-451-4603</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Robert Berg</td>
<td><a href="mailto:Bob.Berg@va.gov">Bob.Berg@va.gov</a></td>
<td>701-239-3754</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Raymond Nelson</td>
<td><a href="mailto:Raymond.Nelson2@va.gov">Raymond.Nelson2@va.gov</a></td>
<td>701-451-7814</td>
</tr>
</tbody>
</table>
Abstract

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

The Area Fargo is an Information Systems Boundary that consists of The Fargo VA Medical Center, The Fargo Veterans Benefits Administration, the Fargo National Cemetery Administration, (10) Community Based Outpatient Clinics (CBOC), (4) Veterans Centers, (2) Annex locations, (1) Home Based Primary Care (HBPC), and (1) Community Resource and Referral Center (CRRC). The systems environment is comprised of workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices and special purpose systems. The system 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.

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 system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- 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
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what
FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.

- 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 CSP or its customers (VA) be affected?

The Area Fargo collects, processes, and/or retains the information of over 30,000 veterans, contractors and VA employee information.

The Midwest District Area was newly created in 2016 when the Office of Information and Technology made major changes to VA systems and their security boundaries. Previously the Area Fargo operated a local area network (LAN) as well as the Private Branch Exchange (PBX). These systems now reside in the GSS information system boundary. All Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) that once resided on the Area Fargo VA LAN and PBX now reside in GSS. This data ownership remains at the facility level and many of the decisions related to the collection, use, storage, and dissemination of the data are made at the facility level.

The Area Fargo staff independently decides whether to share data with other sources as stated throughout this document. The Area Fargo conducts a variety of information sharing internal and external to the Department of Veterans Affairs. Internal sharing is discussing in greater detail in Section 4 of this Privacy Impact Assessment (PIA). This type of sharing is done to ensure that veterans and their families receive the necessary care and benefits. External sharing, which is discussed in greater detail in Section 5 of this PIA is done with other agencies and organizations.

The legal authorities to operate the GSS system are Title 5, United States Code, section 301, Title 38, United States Codes, sections 109, 111, 501, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, and 7105 and Title 38, United States Code, Section 7301 (a).

- Applications for Employment under Title 38, USC-VA, SORN 02VA135
- Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending’s, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records – VA, SORN 14VA05 (November 18, 2010)
- Non-VA Fee Basis Records – VA, SORN 23VA163 (August 31, 2014)
- Patient Medical Records – VA SORN 24VA10P2 (August 14, 2014)
- Veteran, Patient, Employee and Volunteer Research and Development Project Records – VA SORN 34VA12 (May 27, 2010)
- Community Placement Program – VA, SORN 65VA112 (July 9, 2009)
- Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 7VA10P2 (October 31, 2012, as amended)
- Income Verification Records – VA, SORN 89VA10NB (December 19, 2013)
- Automated Safety Incident Surveillance and Tracking System – VA, SORN 99VA13 (March 31, 2009)
Telephone Service for Clinical Care – VA, SORN 113VA112 (May 8, 2009)
The Revenue Program Billing and Collection Records – VA, SORN 114VA16 (December 10, 2009, as amended)
National Patient Databases – VA, SORN 121VA19 (May 11, 2012, as amended)

Section 1. Characterization of the Information

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

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

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

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

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

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial 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)

- Gender as provided by the patient
- Name and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Medical statistics for research purposes containing PII/PHI
- Name and contact information for Next of Kin
- Service Connected rating and disabilities (based on information provided by Veteran and/or VBA)
- Date of death as supplied by Next of Kin or provider
- Criminal background and dependent information as reported by patient and/or national databases

**PII Mapping of Components**

Area Fargo consists of 49 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Area Fargo and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>OITFARSQL001\AUDIOLOGY</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>Federal Information processing Standards (FIPS) 140-2 Advanced Encryption (AES), 256</td>
</tr>
<tr>
<td>OITFARSQL001</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQL001</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQL001</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>Description</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>OITFARSQLO01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAR-WS1270916\CARDIOPERFECT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAR-WS1270916\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>FAR-WS681415\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>FAR-WS681415\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Number, Health Care Information</td>
<td>facilitate patient care</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>VHAFARSQ30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>FAR-WS681427\WSCARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>FAR-WS681427\WSCARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQ001\AUDIOLOGY</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQ001</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQLO01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQLO01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>OITFARSQLO01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>R02FARAPPRPC01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
</tr>
<tr>
<td>Code</td>
<td>Yes/No</td>
<td>Yes/No</td>
<td>Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>--------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>R02FARWEBVRO01</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>FAR-WS1270916\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>FAR-WS1270916\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>FAR-WS681415\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>FAR-WS681415\CARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Social Security Number, Health Care Information</td>
<td>AES256</td>
<td></td>
</tr>
<tr>
<td>Number, Social Security Number, Health Care Information</td>
<td>The data is needed to facilitate patient care</td>
<td>AES256</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VHAFARSQL30</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAR-WS681427\WSCARDIOPERFECT</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**1.2 What are the sources of the information in the system?**

*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 program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system 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 Area Fargo comes from a variety of resources. 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.

Area Fargo also collects data already provided to other organizations within the VA, including:

- Veteran’s Benefit Administration (VBA)
- Austin Automation Center (AAC)
- Health Eligibility Center (HEC)
- Veterans’ Health Administration (VHA)
- Veteran Service Organization (VSO)

Additional data, such as confirmation of military service or results of employee background checks, come from external Federal Agencies. These agencies include:

- Department of Defense (DoD)
- VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers.
- Criminal background information is obtained from Electronic Questionnaires for Investigations Processing (E-QIP)
- National Crime Information Center (NCIC), used to confirm employment and/or volunteer eligibility and to assist VA Police Services while conducting investigations.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system 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.

Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, Request for and Authorization to Release Medical Records Fillable), and via electronic and web form submissions.
Information is also collected from a variety of other IT systems and resources (which is mentioned in Section 4 and 5) internal and external to the VA. 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 SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

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

Much of the information collected is maintained, used, and disseminated by Area Fargo 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.

Employee and VA contractor information is maintained based on Human Resources (HR) and payroll needs and Federal contracting requirements.

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

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

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

Information obtained directly from the individual will be assumed to be accurate. Information may be verified with other Federal agencies (VBA, DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information come to the attention of facility staff, it will be documented and verified prior to further use.

Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center
are obtained. Practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections.

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 system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

This question is related to privacy control AP-1, Authority to Collect

The Area Fargo System is a facility level entity that operates under the authority of Veterans’ Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Applicants for Employment under Title 38, USC-VA, SORN 02VA135 (Prior to 1995) Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending’s, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05 (Nov. 18, 2010)
- Non-VA Fee Basis Records-VA, SORN 23VA10NB3 (July 30, 2015)
- Patient Medical Records-VA, SORN 24VA10P2 (August 14, 2014)
- Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA, SORN 34VA12 (May 27, 2010)
- Community Placement Program-VA, SORN 65VA122 (July 9, 2009)
- Health Care Provider Credentialing and Privileging Records-VA,SORN 77VA10A4 (June 25, 2015)
- Veterans’ Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (Oct. 31, 2012, as amended)
- Income Verification Records-VA, SORN 89VA10NB (December 19, 2013)
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:**
The Area Fargo system contains sensitive personal information – including social security numbers, names, dates of birth and protected health information – on veterans, members of the public, & VA employees and contractors. 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 harm or even identity theft may result.

**Mitigation:**
Veterans Health Administration (VHA), Midwest District Territory 1 as well as Area Fargo deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. Region 2’s security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress.
Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

Due to the extensive amount and nature of the information contained in the Area Fargo, within the Midwest District Territory 1 system boundary, it is impossible to independently list each data point collected and describe its purpose. Below is a description of how different categories of data are used. If you have questions about a certain data point, please contact your facility privacy officer to learn more.

Please review below business purposes to ensure they accurately reflect the facilities’ practices. Include additional information as appropriate.

- **Name:** Used to identify the patient during appointments and patients and employees in other forms of communication.
- **Social Security Number:** Used as a patient and employee 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 calculate travel pay.
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct tele health 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 myHealthVet 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 party health care plans.
- **Certificate/License numbers:** Used to track and verify legal authority to practice medicine and licensure for health care workers in a particular area of expertise.
- **Vehicle License Plate Number:** Used to track vehicles on VA grounds by VA Police to quickly identify vehicle ownership and authorization to be on facility grounds.
- **Internet Protocol (IP) Address Numbers:** Used to track, identify and locate a device on a network and to ensure no two devices are assigned the same IP.
- **Gender:** Used for patient demographic information.
- **Previous Medical Records:** Used for continuity of health care.
• **Current Medications**: Used within the medical records for health care/treatment purposes.
• **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 a representative has been appointed or designated because the patient is unable to make decisions.
• **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. 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.
• **Education information**: Used to determine VA employment eligibility as well as for patient health care/treatment purposes.
• **Medical statistics**: Used for research purposes containing PII/PHI.
• **Date of Death**: Used for death certificate, benefits and memorial honors.
• **Criminal background**: Used to determine VA employment eligibility as well as patient health care/treatment purposes.

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

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

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

Patient and employee data is analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. The Area Fargo uses statistics and analysis to create various reports which provide a better understanding of patient care and employee needs.

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

A complete list of the nationally released Area Fargo Class 1 software packages may be obtained at http://www.va.gov/vdl/.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.
The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

Prior to signing into Area Fargo system users are provided the below banner of Notice to User sign-on:

VA systems are intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized for official business and limited personal use under VA policy.

Information from this system resides on and transmits through computer systems and networks funded by the VA. All access or use constitutes understanding and acceptance that there is no reasonable expectation of privacy in the use of Government networks or systems. All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action including (but not limited to) monitoring recording copying auditing inspecting investigating restricting access blocking tracking disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel.

Unauthorized user attempts or acts to (1) access upload download change or delete information on this system (2) modify this system (3) deny access to this system (4) accrue resources for unauthorized use or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.

Area Fargo staff is trained in specific GSS software based on job duties such as Computerized Patient Record System (CPRS), Scheduling, Billing, etc. Facilities.

**Section 3. Retention of Information**

The following questions are intended to outline how long information will be retained after the initial collection.
3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Area Fargo follows national VA policies regarding information retention. The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- 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
- Gender as provided by the patient
- Name and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Medical statistics for research purposes containing PII/PHI
- Name and contact information for Next of Kin
- Service Connected rating and disabilities (based on information provided by Veteran and/or VBA)
- Date of death as supplied by Next of Kin or provider
- Criminal background and dependent information as reported by patient and/or national databases

3.2 How long is information retained?
In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

When managing and maintaining VA data and records, Area Fargo will follow the guidelines established in VA Record Control Schedule (RCS)-10 (https://www.va.gov/vhapublications/rcs10-1.pdf), as well as RCS 005-1 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf).

These documents specify how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level.

For greater details related to records retention at the Veterans’ Health Administration, please review RCS-10 and RCS-005-1.

Below are some key record retention schedules for your information:

**Medical Records Folder File or CHR (Consolidated Health Record):** These records contain all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a Federal records storage facility. 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, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d. (May 2016)).

**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, Part Two, Chapter Three-Civilian Personnel, Item No. 3000.1 (May 2016)).

**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, Part Two, Chapter Four-Finance Management (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for specific guidelines.

**Office of Information & Technology (OIT) Records:** These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (August 3, 2009). Please refer to VA Records Control Schedule (RCS)-05 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) for specific guidelines.

Additionally, under OMB and NARA guidelines, Area Fargo will reference the Records Management Resources within the General Records Schedule. These specific resources can be found at http://www.archives.gov/records-mgmt/grs/.
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 system owner. 

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

When managing and maintaining VA data and records, Area Fargo will follow the guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS)-10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/)

3.4 What are the procedures for the elimination of SPI?

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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubs

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 Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), https://www.va.gov/vapubs. 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 Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, Area Fargo follows Field Security Service (FSS) Bulletin for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?
Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

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

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

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 system.

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

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that the information maintained by Area Fargo could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.
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 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Benefits Administration (VBA)</td>
<td>Veteran Benefits Information is shared to assist in financial, benefits payment, educational and spousal benefits and service connected disabilities</td>
<td>Pertinent PII, PHI and III including name, SSN, DOB and financial or health information as it pertains to each individual request</td>
<td>Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. VBA employees can log into CPRS via CAPRI, encrypted emails, mail of encrypted CDs,</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Veteran Health Administration</strong></td>
<td>Medical treatment and healthcare services</td>
<td>Patient medical records from internal and external sources</td>
<td>Electronically pulled from VistA through Computerized Patient Record System (CPRS).</td>
</tr>
<tr>
<td><strong>Board of Veterans’ Appeals</strong></td>
<td>Information shared to provide assistance in obtaining benefits for applicants in education, loans, insurance and other</td>
<td>Pertinent PHI or PII appropriate to the request</td>
<td>Information may be transmitted upon request in an electronic, written or verbal format based on the individual request.</td>
</tr>
<tr>
<td><strong>Contractors</strong></td>
<td>Information is shared to assist in financial, benefits payment, educational and spousal benefits and service connected disabilities</td>
<td>Pertinent PII, PHI and III including name, SSN, DOB and financial or health information as it pertains to each individual request</td>
<td>Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Contract VBA employees can log into CPRS via CAPRI, encrypted emails, mail of encrypted CDs, secure facsimile or hard copies via routine mail.</td>
</tr>
<tr>
<td><strong>National Cemetery Administration</strong></td>
<td>Information is shared requesting verification of death benefits</td>
<td>Pertinent PII, PHI, III appropriate to the request</td>
<td>Information may be transmitted upon request in an electronic, written or verbal format based on the individual request.</td>
</tr>
<tr>
<td><strong>Austin Information Technology Center</strong></td>
<td>PII fiscal data</td>
<td>Fiscal data</td>
<td>Software interface</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Direct and Indirect Patient Care Providers</td>
<td>Health/medical payment authorization</td>
<td>Demographics, diagnoses, medical history, service connection, provider orders, VHA recommendation/approval for non-VA care</td>
<td>Fee Basis Claim System authorization software program</td>
</tr>
<tr>
<td>Eligibility and Enrollment Staff</td>
<td>Determine veteran eligibility</td>
<td>Service dates, SSAN, demographics, service connection</td>
<td>Scanned documents uploaded into shared software program</td>
</tr>
<tr>
<td>VA Tumor Register</td>
<td>Tracking and trending diseases</td>
<td>Diagnosis and procedures, tumor status, treatment outcome, survivor tracking, type of treatment, demographics, hormone, radiation, chemotherapy, problems list</td>
<td>Electronic tumor register package</td>
</tr>
<tr>
<td>VA HIV Register</td>
<td>Tracking and trending of disease progression</td>
<td>Diagnosis and procedures, HIV/AIDS status, treatment outcomes, survivor tracking, type of treatment, demographics, problem list</td>
<td>Electronic HIV catalogue package</td>
</tr>
<tr>
<td>VA Network Authorization office for Non-VA Care Payments</td>
<td>Health/medical payment authorization</td>
<td>Demographics, diagnoses, medical history, service connection, provider orders, VHA recommendation/approval for non-VA care</td>
<td>Fee Basis Claim System authorization software program</td>
</tr>
<tr>
<td>VA Health Eligibility Center</td>
<td>Determine veteran eligibility</td>
<td>Service dates, SSAN, demographics, service connection</td>
<td>Scanned documents uploaded into shared software program</td>
</tr>
<tr>
<td>Consolidated Patient Account Center</td>
<td>Medical care cost recovery</td>
<td>Diagnoses, service connection, dates of service, health insurance information, demographics</td>
<td>Electronically pulled from VistA through CPRS</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.

Follow the format below:

**Privacy Risk:** The sharing of data is necessary for the medical care of individuals eligible to receive care at Area Fargo. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

**Mitigation:** The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation. Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

System menus and security keys are assigned by an approved ePAS request based on specific job or duty requirements with least privileges. This access is reviewed for appropriateness on a quarterly basis.

System applies the sensitive record flag to all employees and any veteran record where the veteran requests the record be sensitized. The ISO reviews System audit messages for any potential access abnormalities or violations.

Area Fargo completes a multitude of auditing functions based on VA Handbook 6500 guidelines. Area Fargo completes an in-depth audit of GSS accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as ad hoc reports upon request.

**Section 5. External Sharing/Receiving and Disclosure**

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?
Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties
<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Personnel Management</td>
<td>Activities related to background investigations</td>
<td>Fingerprints and PII as part of PIV screening</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>SSA</td>
<td>Payment/disability benefits</td>
<td>SSN; PHI/PII as described in Section 1.1 of this document as needed organization</td>
<td>Title 38 USC Section 5701, SORN 79VA19</td>
<td>Secure fax and secure web portal</td>
</tr>
<tr>
<td>DOD</td>
<td>Determination of member’s fitness to perform any particular mission, assignment, order, or duty</td>
<td>PII/PHI as described in Section 1.1 of this document as needed by organization</td>
<td>MOU; Privacy Act, 5 USC 552a; Public Law 104-191; 38 USC, 5701, 5705, 7332</td>
<td>Joint Legacy Viewer (JLV); secure web portal</td>
</tr>
<tr>
<td>Center for Disease Control (CDC)</td>
<td>Collaboration with states to provide health care data</td>
<td>Provision of health care reporting PHI/PII as described in Section 1.1 of this document as needed by organization</td>
<td>Standing Letter Request</td>
<td>Secure fax and secure web portal</td>
</tr>
<tr>
<td>Federal Emergency Management Agency (FEMA)</td>
<td>Bed availability status for emergency preparedness</td>
<td>FEMA recovery data may include Identifiable Information (PII) and Sensitive PII (SPII)</td>
<td>VA agreement FEMA/GOFT-1 and FEMA Recovery Policy 9420.1</td>
<td>FEMA website</td>
</tr>
<tr>
<td>Federal Bureau of Investigation (FBI)</td>
<td>Used to confirm employment and/or volunteer eligibility and to</td>
<td>Name, Date of Birth, Sex, SSN, and demographics.</td>
<td>VA SORN 02VA135</td>
<td>Electronic via FBI Website</td>
</tr>
<tr>
<td>Service Provider</td>
<td>Service Description</td>
<td>Data Type</td>
<td>MOU/ISA</td>
<td>Communication Method</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>-----------</td>
<td>---------</td>
<td>----------------------</td>
</tr>
<tr>
<td>VA Police Service</td>
<td>Assist with conducting internal investigations</td>
<td>VA SORN 79A19</td>
<td>Secure fax and secure web portal</td>
<td></td>
</tr>
<tr>
<td>State Prescription Drug Monitoring North Dakota</td>
<td>Prescription information required by State</td>
<td>Protected health care reporting PHI/PII as described in Section 1.1 of this document as needed by organization</td>
<td>National ISA/MOU</td>
<td></td>
</tr>
<tr>
<td>Alaris Carefusion Infusion Pumps</td>
<td>For technical support while troubleshooting malfunctions</td>
<td>No Sensitive Data</td>
<td>National MOU/ISA</td>
<td>Secure Sockets Layer (SSL)</td>
</tr>
<tr>
<td>ALERE</td>
<td>Activities related to system support and patient care.</td>
<td>Clinical data that may contain PHI</td>
<td>National MOU/ISA</td>
<td>Transmitted by means of Site to Site (S2S)</td>
</tr>
<tr>
<td>BAYER</td>
<td>Activities related to system support and patient care.</td>
<td>No Sensitive Data</td>
<td>National MOU/ISA</td>
<td>Transmitted by means of Site to Site (S2S)</td>
</tr>
<tr>
<td>BRIT/Visage Dicom Images</td>
<td>Exchanging data between the BRIT PACS Systems, owned by DVA, and BRIT Systems for the express purpose of providing technical support which will expedite the processing of data associated with remote diagnostics, maintenance, monitoring, and repair by BRIT technical support services for the BRIT PACS</td>
<td>Data includes but is not limited to service specific data to perform remote support; incidental exposure to limited data sets with specific PHI elements depending on application such as patient name, DOB, SSN, Record ID, images and gender; and log files and program updates</td>
<td>National MOU/ISA</td>
<td>Transmitted by means of Site to Site (S2S)</td>
</tr>
<tr>
<td>Systems Installed</td>
<td>Purpose of Interconnection</td>
<td>Sensitive Data</td>
<td>MOU/ISA</td>
<td>Information Transmitted</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>----------------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Ortho-Clinical Diagnostics, Inc</td>
<td>The purpose of the interconnection is for Ortho Clinical Diagnostics staff to access Department of Veterans Affairs (DVA)'s Ortho Clinical Diagnostics Vitros System for blood analysis for remote diagnostics, maintenance, monitoring and repair services.</td>
<td>No Sensitive Data, Software updates and in some instances, assay calibration information</td>
<td>National MOU/ISA</td>
<td>Information may be transmitted by means of Site to Site (S2S).</td>
</tr>
<tr>
<td>PHILIPS</td>
<td>Activities related to system support and patient care.</td>
<td>System Log files, sample clinical data that may contain PHI appropriate to the agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>GETWELL</td>
<td>Activities related to system support and patient care.</td>
<td>System Log files, sample clinical data that may contain PHI appropriate to the agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>SORNA CD/DVD DICOM Burner Devices</td>
<td>Interconnection is needed in order to exchange data between Sorna CD/DVD Production System and Sorna Technical Services Department to expedite processing of data associated with Sorna systems implementation, software, software updates, software code trace files, machine language trace files, network package captures, and DICOM protocol language to assist in the analysis of troubleshooting.</td>
<td></td>
<td>National MOU/ISA</td>
<td>Information may be transmitted by means of VPN IPSEC Tunnel.”</td>
</tr>
<tr>
<td>Company</td>
<td>Activities Related to System Support and Patient Care</td>
<td>System Log Files, Sample Clinical Data That May Contain PHI Appropriate to the Agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site (S2S) VPN Tunnel</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Sysmex America Lab Results</td>
<td>Remote Software Upgrades, Troubleshooting Technical Issues and Maintenance Within Prescribed Timelines</td>
<td>System Log Files, Sample Clinical Data That May Contain PHI Appropriate to the Agreements</td>
<td>National ISA/MOU</td>
<td>Site to Site (S2S) VPN Tunnel</td>
</tr>
<tr>
<td>Topcon</td>
<td>Activities Related to System Support and Patient Care</td>
<td>System Log Files, Sample Clinical Data That May Contain PHI Appropriate to the Agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>VECNA</td>
<td>Activities Related to System Support and Patient Care</td>
<td>System Log Files, Sample Clinical Data That May Contain PHI Appropriate to the Agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>Siemens</td>
<td>Activities Related to System Support and Patient Care</td>
<td>System Does Not Store PHI Data. This Data Is Not Transferred Over the Secure VPN Connection.</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>Roche</td>
<td>Activities Related to System Support and Patient Care</td>
<td>System Log Files, Sample Clinical Data That May Contain PHI Appropriate to the Agreements</td>
<td>National ISA/MOU/BAA</td>
<td>Site to Site VPN Tunnel</td>
</tr>
<tr>
<td>Omnicell</td>
<td>Provides Medicine and Supply Automation Support Services and Technical Support, While Troubleshooting Malfunctions</td>
<td>Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable</td>
<td>National MOU/ISA</td>
<td>Information May Be Transmitted by Means of Site to Site (S2S).</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.

Follow the format below:

**Privacy Risk:**
The sharing of data is necessary for the medical care of individuals eligible to receive care at Area Fargo. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

**Mitigation:**
The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

All personnel accessing Veteran’s information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. A background investigation is required commensurate with the individual’s duties.

Individual users are only given job position specific access to individually identifying data. Access to Area Fargo System requires multi-layer authentication. The individual first must authenticate through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. Area Fargo System access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts.

**Section 6. Notice**

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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 system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that they individual read and understood the NOPP is scanned into each applicant’s electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):


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 Veterans’ Health Administration (VHA) as well as Area Fargo only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide the information, this will prevent them from obtaining the benefits necessary to them.

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

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent
Individuals have the right to consent to particular uses of information. Individuals are directed to use the VA Form 10-5345 Release of Information form describing what and to whom information is being sent.

Individuals can request further limitations on other disclosures (including research). A veteran, guardian or court appointed Power of Attorney can submit a request for restriction to the facility Privacy Officer for processing/review.

Patients have the right to opt-out of the VA facility directory.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk:**
There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans’ Health Administration and Area Fargo prior to providing the information to the VHA.

**Mitigation:**
This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are provided to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. 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 (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.
7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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

Veterans can gain access to their Electronic Health Record (HER) by enrolling in MyHealthVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html.

Veterans and beneficiaries may also request copies of their medical records and other records containing personal data from Area Fargo Release of Information (ROI) office.

Any individual who would like information under the Freedom of Information Act (FOIA) [5 U.S.C. 552] should contact the facility’s FOIA Officer in writing at HAFARFOIAOfficer@va.gov.

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 medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the Privacy Officer at 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 decision to approve or deny is made by the practitioner who entered the data and relayed to the Veteran in writing by the facility Privacy Officer. Appeal rights are provided if a request is denied. The goal is to complete any evaluation and determination within 30 days.
A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the Area Fargo Privacy Officer (PO), or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, 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 Area Fargo business office for processing.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

**Right to Request Amendment of Health Information.**

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

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

Information can also be obtained by contacting the Area Fargo ROI office.

SORNs listed in question 6.1 each discuss and notify members of the public of the procedures related to record access, redress, and correction. Links to all VA SORs can be found at:

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
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 ensure data accuracy.

A formal redress process via the amendment process is available to all individuals as discussed in section 7.2 above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

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

Follow the format below:

Privacy Risk:
There is a risk that individuals whose records contain incorrect information may not receive notification of appointments, prescription medications, or test results. Furthermore, incorrect information in a health record could result in improper diagnosis and treatment.

Mitigation:
As discussed in question 7.3, the Notice of Privacy Practice (N OPP), which every patient receives prior to receiving treatment at the VA, discusses the process for reviewing and requesting an amendment to one’s records. Beneficiaries receive a copy of the NOPP every three years.
The Area Fargo Release of Information (ROI) office is available to assist Veterans with obtaining access to their medical records and other records containing personal information.

The Veterans’ Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features.

In addition, Privacy Handbook 1605.1 establishes procedures for Veterans to have their records amended where appropriate.

**Section 8. Technical Access and Security**

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

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

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

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

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

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

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

Access is requested per Midwest District Territory 1 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

Access to Area Fargo system requires multi-layer authentication. The individual first must authenticate through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. System access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts. Once inside the system, individuals are authorized to access information on a need to know basis. Strict physical security control
measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at Area Fargo is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in Area Fargo system may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from Area Fargo system and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at Area Fargo, or an OIG office location remote from Fargo VAHCS, is controlled in the same manner.

Information downloaded from Area Fargo system and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e. COR, Contracting Officer, Contract Review Committee).

The Privacy Officer is responsible for monitoring all local contracts that require a Business Associate Agreement (BAA). The Privacy Officer will coordinate an annual review all local contracts to monitor the contractor’s compliance with the BAA.

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate
background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA 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 Fargo system access must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees.

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

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

All VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the Area Fargo Privacy Officer and Information System Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

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
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

Please note that all systems containing SPI 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.

Authority To Operate information is ongoing within Risk Vision – The most current Authority To Operate (ATO) memo is dated 4/21/2021

The current FIPS 199 Classification of the Area Fargo is MODERATE.
### 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 System 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>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>Data Minimization and Retention</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>Individual Participation and Redress</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>Security</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>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System 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>Use Limitation</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------</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 Responsible Officials

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

Cheryl L. Asmund
190085

PO, Cheryl Asmund

Robert A Berg
200601

Information Security Systems Officer, Robert Berg

Raymond A Nelson 190583

System Owner, Raymond Nelson
APPENDIX A-6.1

Notice of Privacy Practices (9/30/2019) can be found here:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928