

**Privacy Impact Assessment - 2009 (Form) / Enrollment Enhancements-2009 (Item)**

**Part I. Project Identification and Determination of PIA Requirement**

**1. PROJECT IDENTIFICATION:**

**1.1) Project Basic Information:**

*1.1.a) Project or Application Name:*

Enrollment Enhancements-2009

*1.1.b) OMB Unique Project Identifier:*

029-00-01-11-01-1191-00

*1.1.c) Project Description*

*Project description is pre-populated from Exhibit 300 Part I.A.8. You will not be able to edit the description on this form.*

In October 1996, Congress enacted the Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262, which required VHA to implement a priority-based enrollment system. Enrollment includes functionality to process veterans' applications for enrollment, share veterans' eligibility and enrollment data with all VA health care facilities involved in the veterans' care, manage veterans' enrollment correspondence and telephone inquiries, and support national reporting and analysis of enrollment data. The Health Eligibility Center (HEC) Legacy system handles this functionality. In September 2007, Enrollment System Redesign (ESR) 3.0 will replace the legacy system in order to provide greater flexibility to meet critical requirements on a timely basis, better safeguards to meet security requirements, and improved reliability.

Further enhancements planned for deployment through FY 2012 will provide many improvements to Enrollment. It will reduce the burden on veterans, who are required to submit income data to update their financial assessments annually, by pulling this information directly from the IRS and SSA. Veterans will have the opportunity to apply for health care benefits and manage existing accounts from the comfort and convenience of their own homes with the advent of a secure online Enrollment portal via the world-wide web. Expanded electronic data sharing with other government agencies will mean a more rapid and accurate enrollment and eligibility determination based on a more comprehensive and authoritative data suite. All of these improvements equate to timely and seamless access to healthcare for our veterans.

This project maps to the BRM Health line of business and Access to Care sub-function.

*1.1.d) Additional Project Information (Optional)*

*The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.*

**1.2) Contact Information:**

<b>1.2.a) Person completing this document:</b>	
<b>Title:</b>	Jennifer Renard
<b>Organization:</b>	CACI representing VHA
<b>Telephone Number:</b>	703-455-4024
<b>Email Address:</b>	jennifer.renard@va.gov
<b>1.2.b) Project Manager:</b>	
<b>Title:</b>	Gerry Lowe
<b>Organization:</b>	VHA

<b>Telephone Number:</b>	814-940-6317
<b>Email Address:</b>	gerry.lowe@va.gov
<b>1.2.c) Staff Contact Person:</b>	
<b>Title:</b>	Floretta Hardmon, Privacy Officer
<b>Organization:</b>	Health Eligibility Center of VHA
<b>Telephone Number:</b>	404-235-1306
<b>Email Address:</b>	floretta.hardmon@va.gov

*ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.*

## 2. DETERMINATION OF PIA REQUIREMENTS:

*A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.*

*2.a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?*

Yes

*2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?*

No

*If "YES" to either question then a PIA is required for this project. Complete the remaining questions on this form. If "NO" to both questions then no PIA is required for this project. Skip to section 14 and affirm.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

## Part II. Privacy Impact Assessment

### 3. PROJECT DESCRIPTION:

*Enter the information requested to describe the project.*

*3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.*

The information is collected in order to determine eligibility and enroll veterans for health care services. Additionally, the collected information is used to keep track of the number of veterans who are served in order to project future enrollment needs of veterans.

*3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?*

Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262  
38 U.S.C. Sections 1705, 1710, 1712, and 1722

*3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.*

1,000,000 - 9,999,999

*3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.*

(2) Development/Implementation
3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.
07/2007
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

**4. SYSTEM OF RECORDS:**

The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?

If "No" then skip to section 5, 'Data Collection'.

Yes

4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?

IF "No" then SKIP to question 4.c.

Yes

4.b.1) For each applicable System of Records, list:

(1) The System of Records identifier (number),

89VA19

(2) The name of the System of Records, and

Healthcare Eligibility Records - VA

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).

<http://www.gpoaccess.gov/fr/index.html>

**IMPORTANT:** For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?

Yes

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?

Created for another project or system

If created for another project or system, briefly identify the other project or system.

Enrollment Operations and Maintenance

4.b.4) Does the System of Records Notice require modification?

If "No" then skip to section 5, 'Data Collection'.

Modification of the System of Records is Required

4.b.5) Describe the required modifications.

Current modifications include but are not limited to a change in the SOR number and also the category of records that the SOR covers.

4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.

Explanation:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## PIA SECTION 5

### Project Name

Enrollment Enhancements-2009

### 5. DATA COLLECTION:

#### 5.1 Data Types and Data Uses

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.

*Important Note: Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."*

Yes	<b>Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)</b>
-----	---

Specifically identify the personal information collected, and describe the intended use of the information.

Name, Address, Email Address, Telephone Numbers, Next of Kin Contact, and Emergency Contact.  
To identify individuals and to communicate with individuals about their health benefits. To determine eligibility and enroll veterans for health care services. Additionally, the collected information is used to keep track of the number of veterans who are served in order to project future enrollment needs of veterans.

Yes	<b>Other Personal Information of the Veteran or Primary Subject</b>
-----	---

Specifically identify the personal information collected, and describe the intended use of the information.

, Date of Birth and Death, Gender, Social Security Number, VA claim number,, Marital Status, Employment, Health Insurance, and Financial data (self-reported income, net worth and deductible expenses).  
To identify the veteran and determine eligibility and enroll veterans for health care services.

Yes	<b>Dependent Information</b>
-----	------------------------------

Specifically identify the personal information collected, and describe the intended use of the information.

Spouse and dependent child data including Name, SSN, Date of Birth, Relationship, Address and Date of Marriage or date they became a dependent as well as their employment information, self reported financial information and Federal Tax Information.

To determine eligibility and enroll veterans for health care services.

Yes	<b>Service Information</b>
-----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Branch of Service, Entry Date, Discharge Date, Discharge Type, Military Service Number, Purple Heart, POW, Combat, Exposure to toxic substances while in military, and other military experience related data.  
To determine eligibility and enroll veterans for health care services.

Yes	<b>Medical Information</b>
-----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

VA facility locations where veteran has been provided care. VA diagnostic information is collected if veteran has been determined to be catastrophically disabled

To determine eligibility and enroll veterans for health care services and to share that information with facilities providing care.

No	<b>Criminal Record Information</b>
----	------------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Yes	<b>Guardian Information</b>
-----	-----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

The type, name and address of the veteran's Guardian

To communicate with legal representatives of veterans with a physical or mental problem regarding the veteran's eligibility and enrollment information.

No	<b>Education Information</b>
----	------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

No	<b>Rehabilitation Information</b>
----	-----------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Yes	<b>Other Personal Information (specify):</b>
-----	--

The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

Information about the veteran's eligibility for VA Compensation and Pension benefits.

To determine eligibility and enroll veterans for health care services.

## 5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.

Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)

Note: PIV projects should use the "Other Source(s)" data source.

Yes	<b>Veteran Source</b>
-----	-----------------------

Provide a concise description of why information is collected from Veterans. Provide any required additional, clarifying information.

To identify the veteran, establish records, identify contact information, determine eligibility and enroll veterans for health care services.

No	<b>Public Source(s)</b>
----	-------------------------

i) Specifically identify the Public Source(s) - identify the specific organization(s) or other entity(ies) that supply personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

Yes	<b>VA Files and Databases</b>
-----	-------------------------------

i) Specifically identify each VA File and/or Database that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

VBA through a VHA-initiated Hospital Inquiry (HINQ) - To determine eligibility and enroll veterans for health care services.

Yes	<b>Other Federal Agency Source(s)</b>
-----	---------------------------------------

*i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

SSA for verification of social security numbers of the veteran, and their spouse and dependent children which is required to obtain Federal Tax Information to verify the veteran's eligibility and enrollment. , USPS provides change of address information on veterans with whom VA has corresponded or attempted to correspond with relative to eligibility or enrollment. Change of address information is needed to allow continued communications with veterans about these matters.

No	<b>State Agency Source(s)</b>
----	-------------------------------

*i) Specifically identify each State Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

No	<b>Local Agency Source(s)</b>
----	-------------------------------

*i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Yes	<b>Other Source(s)</b>
-----	------------------------

*i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information.*

Financial institutions and employers – Enrollment sends letters to financial institutions and employers containing federal tax data for independent verification of reported earned and unearned income.

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

### **5.3 Collection Methods**

*Identify and describe how personal information is collected:*

*a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.*

Yes	<b>Web Forms:</b>	Information collected on Web Forms and sent electronically over the Internet to project systems.
-----	-------------------	--

*Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")*

The web version of VA Form 10-10EZ, "Application for Health Benefits", is located at <https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp>. This is the site that veterans access to complete the form. There is a Privacy and Security Statement at [www.va.gov/privacy](http://www.va.gov/privacy) and there is a Notice of Privacy Practices at [http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=1089](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089). There is also a Privacy Statement on the actual 10-10EZ document.

Yes	<b>Paper Forms:</b>	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.
-----	---------------------	--

*Identify and/or describe the paper forms by which data is collected. If applicable, identify standard VA forms by form number.*

VA Form 10-10EZ, which can be printed from the Internet or can be obtained in hard copy from VA Medical Centers.

Yes	<b>Electronic File Transfer:</b>	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.
-----	----------------------------------	--

*Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection – how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)*

VBA provides some eligibility data through a VHA-initiated Hospital Inquiry (HINQ). HINQ provides the capability to request and obtain veteran eligibility data via the VA national telecommunications network. Individual or group requests are sent from a local computer to a remote VBA computer where veteran information is stored. In addition, VBA proactively provides data changes to VHA that could potentially impact a veteran's eligibility for VA health care benefits.

Yes	<b>Computer Transfer Device:</b>	Information that is entered and/or stored on one computer/ system and then transferred to project IT systems via an object
		or device that is used to store data, such as a CD-ROM, floppy disk or tape.

*Describe the type of computer transfer device, and the process used to collect information.*

Computer transfer is done by tape and is restricted to certain data. The Health Eligibility Center verifies veterans' self-reported income based on earned and unearned income data received from the Social Security Administration (SSA) and Internal Revenue Service (IRS). VHA has matching agreements with SSA and IRS.

Yes	<b>Telephone Contact:</b>	Information is collected via telephone.
-----	---------------------------	---

*Describe the process through which information is collected via telephone contacts.*

Veterans provide information via telephone and the information is transferred to the veteran's administrative data stored

in VHA's information systems.

Yes	<b>Other Collection Method:</b>	Information is collected through a method other than those listed above.
-----	---------------------------------	--

*If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.*

VA representatives are the other method used to collect information. The VA representative fills out the VA Form 10-10EZ with the veteran.

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

#### 5.4 Notice

*The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.*

*5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?*

Yes

*Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.*

*5.4.b) Is the data collection mandatory or voluntary?*

Voluntary

*5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?*

It is printed on the VA Form 10-10EZ. Additionally for the web form, there is a Privacy and Security Statement at [www.va.gov/privacy](http://www.va.gov/privacy) and a Notice of Privacy Practices at [http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=1089](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089).

*5.4.d) Is the data collection new or ongoing?*

Ongoing

*5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)*

No	<b>Not applicable</b>
No	<b>Privacy notice is provided on each page of the application.</b>
Yes	<b>A link to the VA Website Privacy Policy is provided.</b>
Yes	<b>Proximity and Timing: the notice is provided at the time and point of data collection.</b>
Yes	<b>Purpose: notice describes the principal purpose(s) for which the information will be used.</b>
Yes	<b>Authority: notice specifies the legal authority that allows the information to be collected.</b>
Yes	<b>Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.</b>

Yes	<b>Disclosures: notice specifies routine use(s) that may be made of the information.</b>
-----	--

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

Yes	<b>Web Forms:</b>
-----	-------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for medical benefits. This and additional privacy information is provided on VA Form 10-10EZ. There is also a Privacy and Security Statement at [www.va.gov/privacy](http://www.va.gov/privacy) and there is a Notice of Privacy Practices at [http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=1089](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089).

Yes	<b>Paper Forms:</b>
-----	---------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for medical benefits. This and additional privacy information is provided on VA Form 10-10EZ.

Yes	<b>Electronic File Transfer:</b>
-----	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c) How a privacy notice is provided?

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for medical benefits. This and additional privacy information is provided on VA Form 10-10EZ.

Yes	<b>Computer Transfer Device:</b>
-----	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c) How a privacy notice is provided?

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for

medical benefits and that VA may verify the information they provide through a computer-matching program. This and additional privacy information is provided on VA Form 10-10EZ.

Yes	Telephone:
-----	------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for medical benefits. This and additional privacy information is provided on VA Form 10-10EZ.

Yes	Other Method:
-----	---------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

VA representatives

Veterans are informed that VA is asking them to provide this information in order for VA to determine their eligibility for medical benefits. This and additional privacy information is provided on VA Form 10-10EZ.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

Complete answer for question "5.4.b) Is the data collection mandatory or voluntary?" Voluntary. However, if veterans do not provide the information to VA, then VA may be unable to process their request for benefits, or the individual may not be able to be enrolled, may have higher out of pocket costs, and may receive limited medical benefits.

### 5.5 Consent For Secondary Use of PII:

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

5.5.a) Will personally identifiable information be used for any secondary purpose?

Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."

No

5.5.b) Describe and justify any secondary uses of personal information.

5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

Some examples of consent methods are: (1) Approved OMB consent forms and (2) VA Consent Form (VA Form 1010EZ). Provide justification if no method of consent is provided.

	Web Forms:
--	------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Paper Forms:</b>
--	---------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Electronic File Transfer:</b>
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	<b>Computer Transfer Device:</b>
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	<b>Telephone Contact Media:</b>
--	---------------------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Other Media</b>
--	--------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

<b>5.6 Data Quality</b>
-------------------------

5.6.a) Explain how collected data are limited to required elements:

For the electronic VA Form 10-10EZ, certain fields are identified as required and veterans are not able to complete the form unless answered, although "none" or N/A is an acceptable response.

5.6.b) How is data checked for completeness?

Designated staff at the VA health care facilities check data for completeness before uploading information into the data file.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?

The data is checked and confirmed using VBA award information.

5.6.d) How is new data verified for relevance, authenticity and accuracy?

Enrollment performs data integrity validation by comparing some data elements against the business requirements encapsulated within the business rule engine to ensure the accuracy and validity of the data elements.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## PIA SECTIONS 6 - 13

### Project Name

Enrollment Enhancements-2009

## 6. Use and Disclosure

### 6.1 User Access and Data Sharing

Identify the individuals and organizations that have access to system data.

--> *Individuals* - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.

--> *Other Agencies* – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.

--> *Other Systems* – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.

6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable items below.

Yes	System Users
-----	--------------

Yes	System Owner, Project Manager
-----	-------------------------------

No	System Administrator
----	----------------------

Yes	Contractor
-----	------------

If contractors to VA have access to the system, describe their role and the extent of access that is granted to them. Also, identify the

contract(s) that they operate under.

There are remote and onsite contractors used in application development of the system. They may have access to the Enrollment data in the execution of their responsibilities.

Several structured mechanisms are used at the system level to ensure that security requirements are incorporated into these operations. All contractors are required to sign rules of behavior for accessed systems and complete IT security and awareness training. VA and VHA Directives 0710 require that all contractor personnel who will be afforded access to sensitive VA systems undergo, at a minimum, an Office of Personnel Management (OPM) background investigation. After the background investigation is completed, it must be favorably adjudicated through the VA Office of Security and Law Enforcement, prior to a contractor being granted system access.

Contractors operate under the Task Life Order (TLO) partnership that supports VHA OI's Health Systems Design and Development (HSD&D). All IT contracts are required to be reviewed at the system level by ISOs and at the enterprise level by VA's Office of Cyber and Information Security (OCIS) to ensure that security requirements are addressed. Contract language is written to require positive background checks, complete mandated training, and comply with VA security policies and procedures for protecting VA's systems and data. Contractors must also follow the VHA IT security rules, which include signing rules of behavior and nondisclosure agreements and completing annual awareness and privacy training modules. This is monitored and verified as part of FISMA compliance reporting. Compliance with the mandated security and privacy training requirements for all employees, volunteers, and contractors is reported to OCIS on an annual basis.

Yes	<b>Internal Sharing: Veteran Organization</b>
-----	---

*If information is shared internally, with other VA organizations identify the organization(s). For each organization, identify the information that is shared and for what purpose.*

The veteran's identifying information, like the Social Security Number, is sent to VBA via a Hospital Inquiry (HINQ) in order to receive eligibility data from VBA.

No	<b>Other Veteran Organization</b>
----	-----------------------------------

*If information is shared with a Veteran organization other than VA, identify the organization(s). For each organization, identify the information that is shared and for what purpose.*

Yes	<b>Other Federal Government Agency</b>
-----	--

*If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.*

Name, Social Security Number, Date of Birth, and Sex are transmitted to SSA in order to verify the social security number (SSN) of the veteran, spouse and dependent children. Verified SSNs are required to verify household members' earned and unearned income information and determine the veteran's eligibility and enrollment

No	<b>State Government Agency</b>
----	--------------------------------

*If information is shared with a State government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.*

No	<b>Local Government Agency</b>
----	--------------------------------

*If information is shared with a local government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.*

--

Yes	<b>Other Project/ System</b>
-----	------------------------------

*If information is shared with other projects or systems:*

*1) Identify the other projects and/or systems, and briefly describe the data sharing. 2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system. 3) For each project and/or system with which information will be shared, describe why information is shared. 4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.*

Basic demographic and eligibility data is shared with a number of VA systems since Enrollment data is essential information about the veteran. These systems include: Pharmacy (Outpatient/Inpatient Pharmacy and CMOP); Billing (Integrated Billing); PIMS (Patient Care Encounters, Event Capture, Scheduling, Ambulatory Care, Patient Transfer Facility program); Computerized Patient Record System; Ancillary Systems (Surgery, Lab, Radiology, Prosthetics); and CAPRI. All integration agreements (API and DBIA) are documented at the VHA level and submitted for approval according to VHA Standard Operation Procedures (SOPs). In addition, it is expected for all users of these systems to have signed security and confidentiality agreements prior to receiving access to each system (as per the VHA SOPs).

Demographic, eligibility, and enrollment data is also sent to VistA so that VA Medical Centers have the information necessary to provide care to the veteran. Users at the medical centers must sign security and confidentiality agreements and receive security and privacy training prior to gaining access to VistA. Also, all ESR data will be stored in the Administrative Data Repository (ADR) database. ADR will be completing a C&A, a Privacy Impact Assessment, and all users will have the same security and privacy training that is required of all VA IT employees and contractors.

ESR will share data bi-directionally with Person Identity Management System (PSIM) and Person Service Demographics (PSD), both of which are part of Common Services. PSIM will be the only authoritative system to manage and maintain veterans' personal information traits within HealtheVet. The veteran's personal identity traits, site of interest, and unique veteran's personal ID will be shared with PSIM. PSD will be the only authoritative system to manage and maintain veterans' demographic information within HealtheVet. The veteran's address and contact information will be shared with PSD. System users will have the same security and privacy training that is required of all VA IT employees and contractors.

Yes	<b>Other User(s)</b>
-----	----------------------

*If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.*

Enrollment sends letters to financial institutions and employers containing federal tax data for independent verification of reported earned and unearned income.

--

*6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:*

System Users, System Owner, Project Manager, Contractor, SSA (Name, Social Security Number, Date of Birth, and Sex are transmitted to SSA), IRS (Social Security Number and the first four characters of the surname are transmitted to IRS).

*6.1.b) How is access to the data determined?*

User access is restricted to the minimum necessary to perform the job and on a need to know basis. All users receive a user ID, password, and access rights as a result of their roles and responsibility to the system. The access by business role is controlled and monitored by the Information Security Officer and the specific roles are defined within the system application.

*6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.*

--

VHA has sharing agreements with the IRS and SSA. Specifically, for the IRS, the agreement is the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Internal Revenue Service". For SSA, the agreement is called the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Social Security Administration". We have an MOU with SSA for the verification of SSNs.

Contractors working for VHA may have access to information. . These contractors are bound by Business Associate Agreements.

6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.

User access is restricted to the minimum necessary to perform the job. Each user is assigned privileges that allow or restrict updating, deleting, and/or inserting records in the database. The system operates so that the user has access only to the information he or she is authorized to access.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

A background investigation is required for all VHA employees filling sensitive positions. VHA personnel and non-VHA personnel have personnel security clearances commensurate with the highest level of information processed by the system.

There are mechanisms in place for holding users responsible for their actions. There are warning banners in place at the log-in screens that describe the consequences if the application is used in an illegal manner, as well as procedures in place for users to report illegal access or illegal use of the information.

Identification and authentication are used to identify and verify the eligibility of a user/process and the rights to access certain information.

Rules for "separation of duties" are practiced on this system. Access privilege controls are documented in AAC Directive 0712 and HEC-18. The access privileges for all users will be granted based on the legitimate and demonstrated need to perform their assigned duties. Only the minimum necessary access to perform authorized business functions will be granted. There is a separation of duties for individuals in sensitive positions.

The system allows the capture of user activities in real-time (e.g., keystroke monitoring).

The HEC User Responsibility Agreement and the AAC User Agreement are both appended to the annual security awareness training conducted at AAC and HEC. Upon the completion of the security awareness training, all AAC and HEC users are required to read and acknowledge the user responsibility agreement.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

Yes

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

All contractors are required to sign rules of behavior for accessed systems and complete IT security and awareness training. VA and VHA Directives 0710 require that all contractor personnel who will be afforded access to sensitive VA systems undergo, at a minimum, an Office of Personnel Management (OPM) background investigation. After the background investigation is completed, it must be favorably adjudicated through the VA Office of Security and Law Enforcement, prior to a contractor being granted system access.

Rules for "separation of duties" are practiced on this system. Access privilege controls are documented in AAC Directive 0712 and HEC-18. The access privileges for all users will be granted based on the legitimate and demonstrated need to perform their assigned duties. Only the minimum necessary access to perform authorized business functions will be granted. There is a separation of duties for individuals in sensitive positions.

All IT contracts are required to be reviewed at the system level by ISOs and at the enterprise level by OCIS to ensure that security requirements are addressed. Contract language is written to require positive background checks, complete mandated training, and comply with VA security policies and procedures for protecting VA's systems and data. Contractors must also follow the VHA IT security rules, which include signing rules of behavior and nondisclosure agreements and completing annual awareness and privacy training modules. This is monitored and verified as part of FISMA compliance reporting. Compliance with the mandated security and privacy training requirements for all employees, volunteers, and contractors is reported to OCIS on an annual basis.

Reference MOU for verification of SSNs,
6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.
SSA, IRS
6.1.i) Describe how personal information that is shared is transmitted or disclosed.
There are remote and onsite contractors used in application development of the system. They may have electronic access to the Enrollment data in the execution of their responsibilities.,
6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.
VHA has matching agreements with the IRS and SSA. Specifically, for the IRS, the agreement is the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Internal Revenue Service". For SSA, the agreement is called the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Social Security Administration". There is also a Memorandum of Agreement between VA and SSA.
6.1.k) How is the shared information secured by the recipient?
IRS protects VHA's information in accordance with Internal Revenue Manual (IRM) 1.16.8, Emergency Planning and Incident Reporting, and 25.10.1 Information Technology (IT) Security Policy and Standards. Records provided by VHA to IRS remain the property of VHA. Records provided to IRS are not used to extract information for any purpose not specified in the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Internal Revenue Service". Additionally, the records are not duplicated or disseminated within or outside the IRS, except as required by federal law, without the written permission of VHA.  SSA protects VHA's information in the same manner in which SSA records are protected under the Privacy Act. Access to the records matched and to any records created by the match are restricted to only those authorized employees and officials who need it to perform their official duties in connection with the uses of the information authorized in the "Computer Matching Agreement for Verification of Income of Medical Care Applicants between Department of Veterans Affairs and Social Security Administration". The records are stored in an area that is physically safe from damage or destruction. They are processed under the immediate supervision and control of authorized personnel in a manner, which will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of computer, remote terminal or other means. They are also transported under appropriate safeguards. All personnel who have access to the records are advised of the confidential nature of the information, the safeguards required to protect the information, and the civil and criminal sanctions for noncompliance contained in applicable federal laws.
6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

<b>6.2 Access to Records and Requests for Corrections</b>	
<i>The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.</i>	
6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by VA? (Select all applicable options below.)	
No	<b>The application will provide a link that leads to their information.</b>
No	<b>The application will provide, via link or where data is collected, written instructions on how to access/amend their information.</b>
No	<b>The application will provide a phone number of a VA representative who will provide instructions.</b>

Yes	<b>The application will use other method (explain below).</b>
No	<b>The application is exempt from needing to provide access.</b>

6.2.b) What are the procedures that allow individuals to gain access to their own information?

Once enrolled, veterans are provided the VA Notice of Privacy Practices, which provides information on accessing and amending data. The Notice is included in the welcome letter and all additional correspondence that is sent to the veteran. The Notice informs the veteran to submit a written request to the VA health care facility that provided the veteran's care.

6.2.c) What are the procedures for correcting erroneous information?

The online 10-10EZ informs the applicants to call their local VA Medical Centers if they want to amend their information. The hard copy 10-10EZ does not provide this explanation. However, since applicants must obtain the hard copy 10-10EZs from their VA Medical Centers and then submit the information to the Medical Centers, they should logically know to contact the Medical Centers to request any changes. Additionally, once enrolled, veterans are provided the VA Notice of Privacy Practices which provides information on accessing and amending data. The Notice informs the veteran to submit a written request to the VA health care facility that maintains the veteran's information.

6.2.d) If no redress is provided, are alternatives available?

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 7 Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

### System of Records Notices may be accessed via:

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

or

[http://vaww.va.gov/foia/err/enhanced/privacy\\_act/privacy\\_act.html](http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html)

For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.

### VHA Handbook 1907.1 may be accessed at:

[http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=434](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434)

For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.

Start by looking at the <http://www.warms.vba.va.gov/20rcs.html>

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic

medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Tapes received from SSA and IRS are destroyed 30 days after the data have been validated as being a true copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Regardless of the record medium, no records are retired to a Federal records center.

7.b) What are the procedures for eliminating data at the end of the retention period?

Depending on the record medium, records are destroyed by either shredding or degaussing.

7.c) Where are procedures documented?

Healthcare Eligibility Records - VA (89VA19) as set forth in Federal Register Vol. 66, No. 97.

7.d) How are data retention procedures enforced?

By following the standards approved by the Archivist of the United States, National Archives and Records Administration, and published in the VHA Records Control Schedule 10-1.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

### 8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:

Authorized web services staff monitors the security log regularly to detect any instance of unauthorized transaction attempts.

All attempts to access and use this system and/or its resources are subject to keystroke monitoring and recording.

Cameras at the HEC are strategically positioned to monitor activities 24 hours per day.

The system's electrical power is monitored.

The computer room is environmentally protected with air conditioning equipment, air filters, fire protection, power regulation with surge suppressers and raised floors. These environmental systems are monitored 24 hours a day, 7 days a week.

System performance monitoring is used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes.

Intrusion detection components are applied throughout the system. IDS monitoring is conducted on a 24 X 7 basis.

8.1.c) Is adequate physical security in place to protect against unauthorized access?

Yes

## 8.2 Project-Specific Security Measures

8.2.a) Provide a specific description of how collected information will be secured.

• A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.

• A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).

• A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.

• Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? If so, describe these controls.

Many controls are in place to secure the Enrollment data. The Security Plan and the Contingency Plan will document all of these controls and procedures in detail.

Enrollment administrative controls include: a risk assessment, vulnerability scanning, a security plan, rules of behavior, software usage restrictions, properly licensed software, configuration management, security testing, certification and accreditation, security assessments, a POA&M, and system monitoring.

Enrollment operational controls include: personnel screening, access privilege controls, personnel sanctions, multiple physical and environmental protection controls, contingency planning and training, alternate storage and processing sites, system backup and recovery, system integrity policy and procedures, media protection and disposal, incident response procedures and training, and security awareness and training.

Enrollment technical controls include: user identification and authentication, user account management, separation of duties, least privilege controls, unsuccessful login attempt controls, system use notification and warnings, audit trails and reporting, and communication protections.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

The project follows the guidance published by the CIO's Office of Cyber and Information Security (OCIS), which establishes directives, policies, and procedures which are consistent with the provisions of the Federal Information Security Management Act (FISMA) and other related federal laws, as well as guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

## 9. CHANGE RECORD

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, n/a: first PIA)

No

If no, then proceed to Section 10, "Children's Online Privacy Protection Act."

If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

• For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

*New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;*

*Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);*

*New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;*

*Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:*

- For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

*Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);*

List All Major Project/System Modification(s)	State Justification for Modification(s)	*Concisely describe:	Modification Approver	Date

\* The effect of the modification on the privacy of collected personal information

\* How any adverse effects on the privacy of collected information were mitigated.

## 10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

10.a) Will information be collected through the Internet from children under age 13?

No

If "No" then SKIP to Section 11, "PIA Considerations".

10.b) How will parental or guardian approval be obtained.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 11. PIA CONSIDERATIONS

11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.

Privacy has always been an important consideration for Enrollment. However, a Privacy Impact Assessment was not completed until after the commencement of the Enrollment project. Therefore, choices regarding this project were not made as a result of performing a Privacy Impact Assessment.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

**12. PUBLIC AVAILABILITY**

*The Electronic Government Act of 2002 requires that VA make this PIA available to the public. This section is intended to provide documented assurance that the PIA is reviewed for any potentially sensitive information that should be removed from the version of the PIA that is made available to the public.*

*The following guidance is excerpted from M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Section II.C.3, "Review and Publication": iii. Agencies must ensure that the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).*

*1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment<sup>9</sup>. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).*

*2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.*

*12.a) Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?*

No

*12.b) If yes, specify:*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

**13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:**

*13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the development time and cost of this project and must be planned for accordingly. I will ensure that VA privacy and information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.*

Yes

*13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)*

Gerry Lowe 5/21/2007

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*