

**Privacy Impact Assessment - 2009 (Form) / Health Admin Center (HAC)  
IT Operations-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:*

Health Admin Center (HAC) IT Operations-2009

*1.1.b) OMB Unique Project Identifier:*

029-00-01-01-01-1040-00

*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.*

HAC provides a variety of critical programs mandated by Congress and delivers quality services to veterans and their family members. HAC's IT operations are closely linked with the business and support the Center's goals through the use of leading IT solutions. The 3 key components of these operations that this project supports are: (1) telecom support; (2) technical support and; (3) purchase and maintenance of capital equipment. HAC IT operations are considered "steady state." The objective of the HAC is to be the VA expert in health plan management with a mission to efficiently administer health plans. The HAC establishes benefits policy, determines eligibility, processes claims and checks for fraud, waste and abuse. The role of the HAC has expanded from its original mission of supporting the CHAMPVA to also include administration of the Department's Foreign Medical Program, Spina Bifida Healthcare Program, Children of Women Vietnam Veterans Health Care Program, VA Diagnostic Related Grouping Recovery Audit, and VHA Mail Management Office. HAC's IT operations have also expanded to meet the broader role to support its mission. These operations are required to support the HAC's automated claims processing system, the eligibility and authorization systems, the call center, interactive intranet and internet web pages for beneficiaries and providers and various other HAC activities. IT operations assist the HAC with administrative functions that are provided to several VHA CFO Field Offices and to the Health Enrollment Center in Atlanta. The focus of this project is maintaining and enhancing the three key components of HAC's IT operations: (1) Telecom Support-The HAC IT telecom component includes the establishment and maintenance of a call center that handles all beneficiary inquiries. Telecom links to the Department of Defense (DoD), Centers for Medicare and Medicaid Services (CMS), EDI clearing houses, VA Medical Centers (support of the CHAMPVA in-house Treatment Initiative (CITI) program) and with the Consolidated Mail Out Pharmacy (Meds by Mail Program). (2) Technical Support: IT technical assistance is necessary to support many HAC systems, including: Claims processing system, Eligibility and authorization systems, Comprehensive intranet/internet websites for stakeholders - (3) Purchase & Maintenance of Capital Equipment: HAC IT department continually upgrades and improves the capital equipment assets to support the HAC's mission and various programs.

*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>	Tom Wayburn
<b>Organization:</b>	VHA Health Administration Center (741)
<b>Telephone Number:</b>	303-370-7757
<b>Email Address:</b>	Thomas.Wayburn@va.gov

<b>1.2.b) Project Manager:</b>	
<b>Title:</b>	Joe Williams
<b>Organization:</b>	VHA Health Administration Center (741)
<b>Telephone Number:</b>	720-889-2346
<b>Email Address:</b>	joseph.williams@va.gov
<b>1.2.c) Staff Contact Person:</b>	
<b>Title:</b>	Joe Williams
<b>Organization:</b>	VHA Health Administration Center (741)
<b>Telephone Number:</b>	720-889-2346
<b>Email Address:</b>	joseph.williams@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.

Information in this system is collected for the purposes of establishing and monitoring eligibility to receive VA benefits and processing medical claims for payment for entitled veterans and beneficiaries.

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

Title 5 U.S.C. 301, Title 38 U.S.C. 501(a), 501(b), 1703, 1724, 1725, 1728, 1781, 1802, 1803, 1813, and PL 103-446, Section 107.

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.
100,000 - 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.
(3) Operation/Maintenance
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.
1988
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

<b>4. SYSTEM OF RECORDS:</b>
<i>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 &amp; Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.</i>
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),
54VA16
(2) The name of the System of Records, and
Health Administration Center Civilian Health and Medical Care Records - VA
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
VA Privacy Act Issuances ( <a href="http://www.gpoaccess.gov/privacyact/index.html">http://www.gpoaccess.gov/privacyact/index.html</a> )
<b>IMPORTANT:</b> 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 specifically for this project
If created for another project or system, briefly identify the other project or system.
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.
SOR needs updated to reflect the April 2006 physical relocation of the HAC. Specifically, the System Location, System Manager Address, and Notification Procedure sections of the SOR must be updated to the current physical address for the facility.

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.

Not Applicable

Explanation:

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

## PIA SECTION 5

### Project Name

Health Admin Center (HAC) IT Operations-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, telephone number, email address, VA file number, narrative description of rated VA service-connected disabilities, social security number, gender, date of birth, date of death, and other direct personal information that may be required, is used to determine eligibility and entitlement to VA medical benefits, for identification purposes, and to communicate with the individual regarding benefits.

No	<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.

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

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

Name, address, telephone number, email address, social security number, date of birth, date of death, other health insurance information, date of marriage or dependency, date of divorce, and other direct personal information that may

be required is used to determine initial and continued eligibility for VA medical benefits, for identification purposes, and to communicate with the individual regarding benefits.

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

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

The veteran's branch and dates of service, and type of discharge is used to verify veteran and dependent status for VA medical care.

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

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

Individual health information, such as name and address of the health care provider, vendor information, billing data, description of services including diagnostic and procedure data, amounts billed, amounts paid, supporting documentation for medical services requiring certification or clarification, and other information that may be required is used to authorize or process medical service claims for VA payment consideration.

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.*

Name and address of an individual's legally appointed guardian or fiduciary is used for communication purposes for beneficiaries who are incapacitated due to a defect in age, mental status, or physical condition.

Yes	<b>Education Information</b>
-----	------------------------------

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

Name and address of the educational institution attended and dates of attendance for CHAMPVA program beneficiaries aged 18-23 is used for the purpose of determining initial and continued eligibility for medical care at VA expense.

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

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

--	--

No	<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.)

## 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.

Identifying, demographic, military, and health information is obtained from the person, or individual legally authorized to act in his or her behalf, who applies for program benefits.

Yes	<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.

Health information may be obtained from health care providers, health plans, and allied health professionals, organizations, and entities for the purpose of coordinating health care services or payment consideration for services.

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.*

Veteran and dependent information may be obtained from Department of Veterans Affairs (VA) Veterans Benefits Administration files and inquiry systems. Billing information may be obtained from VA Veterans Health Administration Medical Centers and facilities for program recipients who obtain their medical services. Payment and accounting information may be obtained from VA data repositories and processors, such as the VA Austin Automation Center (AAC).

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.*

Information about applicants and program recipients who are eligible to receive medical benefits administered by other Federal programs may be obtained from Department of Defense, Centers for Medicare and Medicaid Services, Department of Labor, and Department of State to determine eligibility for program services or to coordinate payment for program services. Payment information is obtained from the Department of Treasury regarding HAC payments authorized for program recipients.

Yes	<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.*

Information from State Department of Medicaid and other public health assistance programs may be obtained for coordination of benefits.

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.*

No	<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.*

**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.")

HAC maintains a web site that collects individually identifiable information used to proof the registrant's identity for the purpose of granting access to an online account containing his or her program eligibility and claim information. The URL for HAC Online is [https://www.va.gov/hac/ciw/ciwmail/ciwb\\_510\\_regclm.asp](https://www.va.gov/hac/ciw/ciwmail/ciwb_510_regclm.asp) and the URL for the associated Privacy and Security notice is <http://www.va.gov/privacy>

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.

Individual information for CHAMPVA applicants is obtained using VA Form 10-10d and via individual correspondence for FMP program applicants. An individual's other health insurance information is collected using VA Form 10-7959c. Individual requests for direct reimbursement for claimed services is obtained using VA Forms 10-7959a and 10-7959e. Mail-out pharmacy information is obtained using VA Form 10-0426. A request for information disclosure is obtained using VA Form 10-5345.

No	<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.)

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.

Individual information pertaining to individuals awarded VA Spina Bifida compensation benefit is collected from VA VBA Regional Office, Hines, IL., via computer transfer media for the purpose of enrolling these individuals for VA medical services benefit.

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

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

Some information in the system is obtained as a result of program beneficiaries and health care providers contacting HAC by telephone, via the toll-free customer call center, and by fax. The purpose of telephone calls is generally customer service related, for example, policy advisement, benefit explanation, precertification requests, and complaint intake. HAC does not solicit information by telephone although some information volunteered by the caller during a telephone conversation may be recorded, such as an address change or returned payment information.

No	<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.

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?

A privacy statement is attached to each form used in the collection of individually identifiable information.

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:</b> notice describes the principal purpose(s) for which the information will be used.
Yes	<b>Authority:</b> notice specifies the legal authority that allows the information to be collected.
Yes	<b>Conditions:</b> notice specifies if providing information is voluntary, and effects, if any, of not providing it.
Yes	<b>Disclosures:</b> notice specifies routine use(s) that may be made of the information.

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

VA Forms Office and OMB approve the web form used to collect data. The Privacy Notice is provided by link to the VA approved web site.

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.

The web page provides an electronic link to the VA Privacy and Security Notice.

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.

A statement providing the authority and reason for data collection, the purpose of collection, and possible disclosures of the information is provided on all forms used to collect information. A Privacy Act statement and Paperwork Reduction Notice is provided as an attachment on forms.

No	<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?

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?

A statement providing the authority and reason for data collection, the purpose of collection, and possible disclosures of the information is provided on the form used to collect the information, OMB approved VA form 21-0304. A Privacy Act and Paperwork Reduction Notice is provided on the form. This information is stored in VA System of Records 58VA21/22 by the collecting department.

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.

HAC does not solicit information from individuals by telephonic means, however information volunteered by individuals during telephone conversations may be captured, such as address updates, changes in insurance information, returned payment data, etc. Individuals are verbally advised that information they voluntarily provide will be accepted and their records updated. A privacy notice is not issued however, as there is no collection or solicitation of information conducted by HAC.

No	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.

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

### 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.)

## 5.6 Data Quality

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

Data collected is restricted only to that personal information used in the determination of eligibility and in the administration of program benefits. Request for information is reviewed by subject matter experts and policy analysts to determine relevancy.

5.6.b) How is data checked for completeness?

Automated controls are in place to ensure that all information needed to make program determinations is captured. The IT system is programmed not to issue benefit award unless all data elements needed for determining the award are complete.

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

Data required to properly administer benefits is validated with the record subject by personal contact or via use of a VA Form, for example, indication of other health insurance information is certified annually using VA Form 10-7959c. Personal data that is used to determine continued eligibility for program benefits is verified annually with the data source, for example, dependency status is verified with the designated VA Regional Office using VA Form 10-3884a. Due process is granted individuals identified with a data discrepancy that may effect the award or provision of benefits.

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

Request for information is reviewed by subject matter experts and policy and procedures analysts to determine relevancy. Information is obtained and verified directly from the applicant or recipient, or validated with the recipient if it adversely effects benefit determination.

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

## PIA SECTIONS 6 - 13

### Project Name

Health Admin Center (HAC) IT Operations-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
-----	-------------------------------

Yes	<b>System Administrator</b>
-----	-----------------------------

Yes	<b>Contractor</b>
-----	-------------------

*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.*

Personal identifiers (name, address, social security number) and eligibility data is shared with private organizations under contract to provide healthcare benefits to program enrollees. Certain contractors have access to data in the system. Information is shared with: \* Mental Health Certification and Reviewer for the purpose of determining mental health benefit coverages for program subscribers. \* Pharmacy Benefit Manager for the purpose of coordinating pharmaceutical services to program subscribers. \*HIPAA ETCS clearinghouse for the purpose of exchanging HIPAA required ETCS from /to covered entities.

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.*

HAC shares the name, social security number, and other identifying personal information, as well as claim, payment and indebtedness data to:  
 \* VA Debt Management Center for the purpose of collecting debts by set off for individuals indebted to the United States.  
 \* VA Veterans Benefits Administration for the purpose of verifying and obtaining information needed to establish or retain eligibility for program benefits for applicants and existing registrants.  
 \* VA Veterans Health Administration healthcare facilities for the purpose of coordinating program benefits for individuals furnished medical services.  
 HAC shares data with these organizations but none of them have access to the system.

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.*

The name, social security number, relationship, date of eligibility, claim and payment data for individuals may be shared with:  
 \* Department of Defense, Defense Enrollment and Eligibility Reporting System, to update their database to identify CHAMPVA program recipients for the purpose of coordinating Federal health plan benefits between the two agencies.  
 \* Centers for Medicare and Medicaid Services for the purpose of validating and obtaining Medicare information needed to establish eligibility for program benefits.  
 \* Department of Defense, TriCare Management Authority, to coordinate eligibility for the other program.  
 \* Department of Treasury for the purpose of processing payments or collecting debts.  
 HAC shares data with these organizations but none of them have access to the system.

No	State Government Agency
----	-------------------------

*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	Local Government Agency
----	-------------------------

*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.*

No	Other Project/ System
----	-----------------------

*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.*

No	Other User(s)
----	---------------

*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.*

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

Only HAC employees and HAC contract employees have direct access to individual information in the system. Access is limited to that information needed to satisfactorily perform responsibilities.

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

Access to individual information is role-based, with access to applications based upon the person's position responsibilities as determined by his or her direct supervisor. Information disclosed to external entities, for example information disclosed to Other Federal Agencies, is done on a data-sharing basis only and by written agreement in accordance with Federal confidentiality statutes. External entities have no direct access to information in the system.

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

HAC abides by VA policy and procedure in granting user access to individual information. Specific policies and procedures enforced are published by the department's Office of Cyber and Information Security, NIST Guidelines, and OMB Circular A-130. HAC also has local privacy and security policies, IS-03 Automated Systems Security Policy, SE-02 HAC Privacy Policy, and the HAC contingency site plan.

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

User access to information is restricted by menu controls to only that data determined relevant and necessary to perform job duties.

*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)*

Prior to gaining computer access, users receive training regarding misuse of data, and sign a Computer Rules of Behavior agreement. Refresher training is also provided. In addition, upon sign-on to the computer system, users must agree with terms listed in a warning banner, which includes language regarding misuse of data. HAC Policy Memo IS-03 addresses data misuse. Fine Grain Access controls are also in place, which give system administrators the ability to control user access to sensitive information.

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 employees are required to take privacy and security training

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.

HAC enters into written agreement, either by contract or Memorandum of Understanding, upon each instance in which individually identifiable information in the HAC system is shared. These agreements contain provisions that bind the other party to federal confidentiality and information security requirements.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.

Data in this system is primarily disclosed to third parties by document reproduction and mailing, but it may be shared electronically via media, such as CD-ROM, disk, and tape.

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.

Routine use

6.1.k) How is the shared information secured by the recipient?

Each recipient of data from this system enters into written agreement to secure the data in accordance with VA policy and requirements.

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?

Recipients of protected health information are required to train workforce members regarding VHA Privacy Policy and VA Information Security training. A HIPAA compliant business associate agreement is enacted whenever individually-identifiable information is shared with other organizations. Per the business associate agreement the contractor is allowed to either complete VA privacy training or privacy training supplied by their company.

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

## 6.2 Access to Records and Requests for Corrections

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.

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	The application will provide a link that leads to their information.
No	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
No	The application will provide a phone number of a VA representative who will provide instructions.
Yes	The application will use other method (explain below).
No	The application is exempt from needing to provide access.

6.2.b) <i>What are the procedures that allow individuals to gain access to their own information?</i>
An individual may request access to the record by submitting written request using VA Form 10-5345a. An appointment with the individual. Following identification proofing, the individual may review the record in a private setting in the presence of the facility Privacy Officer.
6.2.c) <i>What are the procedures for correcting erroneous information?</i>
The individual submits a written notice identifying any inaccurate, untimely, or irrelevant information contained in the record, and describes his or her preferred remedy. The request is reviewed, and a determination made to grant or deny the individual's request. The determination is communicated to the individual. If the request is granted, the record is amended and notice provided to previous recipients of the information.
6.2.d) <i>If no redress is provided, are alternatives available?</i>
If an individual's request for record amendment is denied, he or she may appeal the determination to VA General Counsel. The individual's written response to the alleged inaccurate information is incorporated into the record, and it is enclosed whenever disclosure is made of the contested information.
6.2.e) <i>Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.</i>
Notice of Access and Amendment process is published in the System of Records notice for this system, 54VA16.
<i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i>

## 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.
<b>System of Records Notices may be accessed via:</b>
<a href="http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm</a>
or
<a href="http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html">http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html</a>
For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.
<b>VHA Handbook 1907.1 may be accessed at:</b>
<a href="http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434">http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434</a>
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.
<a href="http://www.warms.vba.va.gov/20rcs.html">Start by looking at the http://www.warms.vba.va.gov/20rcs.html</a>

7.a) <i>What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.</i>
Paper documents are imaged and maintained in the IT system. The disposition schedule is to destroy electronically stored information six years after all individuals in the record become ineligible for program benefits. The paper source documents are destroyed after successfully scanned to electronic medium. Individually-identifiable information shared with other systems is destroyed by the other party upon satisfaction of need and in accordance with the terms of the contract/agreement.
7.b) <i>What are the procedures for eliminating data at the end of the retention period?</i>
Paper documents, including duplication of imaged documents, are shredded. Selected destruction methods comply with

NCSC-TG 025 Version-2/VA Policy. If a degausser is not available, the media is destroyed by smelting, pulverization or disintegration. VA Form 0751 is used to certify and report destruction. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

7.c) Where are procedures documented?

The disposition authority is documented in Section XXXVIII, VHA Record Control Schedule 10-1. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version-2/VA Policy, VA Form 0751, Information Technology Equipment Sanitization Certificate. HAC local policy is documented in IS-03, Automated Systems Security Policy.

7.d) How are data retention procedures enforced?

No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority, such as RCS 10-1. Archived and retired records are maintained in accordance with VA Policy. Certificate of record destruction is maintained by the Records Control Officer.

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:

Certification and Accreditation of all VA information system is required to be completed every three years in order to maintain Full Authority to Operate.

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.
<ul style="list-style-type: none"> <li>• 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?</li> </ul>
<p>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.</p>
<p>Per HAC IS-03 Automated Information Security, user access will be controlled and limited by OCIO based on positive user identification. Authentication mechanisms support the minimum requirements of access control, least privilege, and system integrity for all platforms. Logical access controls are employed to permit only authorized access to the system and restrict users to authorized transactions, functions, and data. These controls ensure that only authorized individuals gain access to information system resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable for their actions. This facility undergoes periodic technical and non-technical IT security reviews, both internal and external. The results of all reviews/audits are securely maintained. This facility has established a set of rules that describes the security operations of the information system and clearly delineates security responsibilities and expected behavior of all system owners, users, operators, and administrators. The rules include the consequences of inconsistent behavior or non-compliance. The rules include all significant aspects of information system use, including policy on use of electronic mail. The entire workforce of this facility will have access to a copy of these rules of behavior for review. A signed acknowledgement of these rules is a condition of access.</p>
<p>8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.</p>
<p>Per HAC IS-03 Automated Information Security, user access will be controlled and limited by OCIO based on positive user identification. Authentication mechanisms support the minimum requirements of access control, least privilege, and system integrity for all platforms. Logical access controls are employed to permit only authorized access to the system and restrict users to authorized transactions, functions, and data. These controls ensure that</p>

<p><b>9. CHANGE RECORD</b></p>
<p>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.</p>
<p>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)</p>
<p>No</p>
<p>If no, then proceed to Section 10, "Children's Online Privacy Protection Act."</p>
<p>If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:</p>
<p>Conversions - when converting paper-based records to electronic systems;</p>
<p>Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;</p>
<p>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:</p>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<p>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:</p>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<p>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;</p>
<p>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);</p>
<p>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;</p>
<p>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:</p>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>

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.

None.

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)

Joe Williams; 09/26/2007

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