

Privacy Impact Assessment - 2009 (Form) / Allocation Resource Center(ARC)-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:

Allocation Resource Center(ARC)-2009

1.1.b) OMB Unique Project Identifier:

029-00-01-01-01-1021-00-110-247

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.

The VHA instituted the VERA system in April 1997. Information Technology (IT) used to gather and analyze VHA data have been cornerstone components of allocation models since the inception of the ARC. VERA ensured that the funds were equitably distributed based on veterans who use the VHA health care system rather than being based on historic funding patterns. VERA has been, and will continue to be, a critical component of VA's success in closing performance gaps related to resource allocation while helping to implement the mission and vision of the VHA. For example by ensuring fair and adequate funding availability, the ARC contributes to strategic quality of life goals such as enhancing the ability of VA to serve returning soldiers as they transition to civilian life and supporting desirable outcomes through informed decision making in the health care arena.

ARC staff provide technical and analytical services supporting the VHA CFO's ability to: develop, implement, and maintain resource allocation methodologies; gather and report on financial aspects of patient workload and cost; classify patients based on care and diagnosis rendered; train and provide information to management officials throughout VA. Without this information, VHA would not be capable of measuring costs or efficiencies. In addition, without this information the VHA would need to depend on alternative funding models such as a historical model. As the VERA model was developed with incentives for improved efficiency, this could undo some of the progress made over the past few years.

Patient workload and cost is gathered from the 156 hospitals, 135 nursing homes, 43 domiciliaries, and numerous community-based outpatient clinics. The ever-increasing volumes of data gathered at these various locations are made available to the ARC via remotely owned and operated IT systems. The data are collected, integrated, analyzed and published using ARC IT systems. It would not be possible for the ARC to track and predict workload and costs without information technology. At an aggregate level the ARC currently produces 751 types of reports consisting of over 7500 detailed monthly reports, 474 detailed quarterly reports and 47 detailed annual reports at the national, VISN and station level. In addition, the ARC provides approximately 300 ad hoc reports and responds to just under 3000 requests each year.

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:

1.2.a) Person completing this document:	
Title:	Dave Pike
Organization:	Same as 1.B.2
Telephone Number:	
Email Address:	
1.2.b) Project Manager:	

Title:	David Pike PMP
Organization:	Allocation Resource Center
Telephone Number:	781-849-1837 ext 125
Email Address:	david.pike@va.gov
1.2.c) Staff Contact Person:	
Title:	
Organization:	
Telephone Number:	
Email Address:	

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

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

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.

To build patient specific cost and workload structures for the VHA Office of Finance. VHA Office of Finance Veterans Equitable Resource Allocation System depends on specific patient cost and workload information to determine where

workload is being generated and at what cost to ensure the equity of resource distribution to VHA networks.
3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?
Routine Uses of data collected under title 38 authority. The use of this data is mandated to provide equitable budgetary and financial functions for VHA services.
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.
(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.
September, 1983
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

4. SYSTEM OF RECORDS:
<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 & 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),
121VA19
(2) The name of the System of Records, and
National Patient Databases- VA
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
The official sites are located at http://vawww.vhaco.va.gov/privacy/Update_SOR/SOR121VA19.pdf , however, the information can also be found at: http://a257.g.akamaiitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/pdf/04-7821.pdf or http://a257.g.akamaiitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/04-7821.htm
<i>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.</i>
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.
VHA uses data stored in national patient databases to prepare

various management, tracking, and follow-up reports necessary for the effective operation of VHA as it plans for and then delivers quality health care.

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 NOT Required.

4.b.5) Describe the required modifications.

N/A

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

Allocation Resource Center(ARC)-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	Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)
-----	---

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

Veterans' social security numbers are used by the National Patient Databases as a unique identifier. In addition, Zip code is used by the National Patient Databases for association with medical facilities.

No	Other Personal Information of the Veteran or Primary Subject
----	---

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

No	Dependent Information
----	------------------------------

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

Yes	Service Information
-----	----------------------------

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

Period of service is maintained within the National Patient Databases and is used by the ARC to respond to associated inquiries from stake holders.

Yes	Medical Information
-----	----------------------------

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

The information is used for health care operations. Patient specific workload information is used to classify individuals into one of 53 patient classes in accordance with the VERA classification rules. The workload information is in the form of procedures (e.g. CPT codes), diagnosis (e.g. ICD9 codes), and utilization (e.g. treating speciality, days of care, clinic stops, RUG scores, dialysis treatments, and medications). The data reviewed includes diagnosis (e.g. DCG codes), procedures (e.g. CPT codes), and utilization (e.g. Bed Days of Care, pharmaceuticals, RUG codes, treating specialties, clinic stops and so forth) information. Classification is an annual process used to aggregate all patients receiving care into specific classes based upon clinical and utilization criteria. The care must be provided or paid for by VHA. Each year, every patient is placed into the single highest class on the patient hierarchy chart that best describes the total care received during the fiscal year. These 53 classes are then rolled up into 10 price groups for the purpose of distributing funds to VISNs. For the VERA 2004 model, the price for each of the VERA 10 Price groups is based on the national average cost of caring for the patients in each Price Group and the President's budget. Cost information is integrated with workload information to determine patient specific costs. These costs are used to prorate patients that are seen at multiple VISNs (Prorate Patients or PRPs). Historical PRPs function as a data-driven decision making tool. They are also used to predict future VISN resource needs.

No	Criminal Record Information
----	------------------------------------

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

No	Guardian Information
----	-----------------------------

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

No	Education Information
----	------------------------------

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

Yes	Rehabilitation Information
-----	-----------------------------------

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

The information is used for health care operations. Patient specific workload information is used to classify individuals into one of 53 patient classes in accordance with the VERA classification rules. Data collected in this case includes diagnosis codes (ICD9), RUG scores, treating specialties and utilization (days of care).

The data reviewed includes diagnosis (e.g. DCG codes), procedures (e.g. CPT codes), and utilization (e.g. Bed Days of Care, pharmaceuticals, RUG codes, treating specialties, clinic stops and so forth) information.

Classification is an annual process used to aggregate all patients receiving care into specific classes based upon clinical and utilization criteria. The care must be provided or paid for by VHA. Each year, every patient is placed into the single highest class on the patient hierarchy chart that best describes the total care received during the fiscal year. These 53 classes are then rolled up into 10 price groups for the purpose of distributing funds to VISNs. For the VERA 2004 model, the price for each of the VERA 10 Price groups is based on the national average cost of caring for the patients in each Price Group and the President's budget. Cost information is integrated with workload information to determine patient specific costs. These costs are used to prorate patients that are seen at multiple VISNs (Prorate Patients or PRPs). Historical PRPs function as a data-driven decision making tool. They are also used to predict future VISN resource needs.

Yes	Other Personal Information (specify):
-----	--

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.

Enrollment data is captured for the purpose of providing national reports and influencing the allocation system. Summary information is also posted to a Web Site to assist VHA networks and facilities to monitor their workload reporting and cost assignments.

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.

No	Veteran Source
----	-----------------------

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

No	Public Source(s)
----	-------------------------

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	VA Files and Databases
-----	-------------------------------

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.

For the purpose of patient classification and costing, data is collected from the following Veterans Affairs data sources: Patient Treatment File (treating specialty, ICD9 codes and days of care); National Patient Care Database (clinic stops, CPT codes); Resident Assessment Instrument/Minimum Data Set (RUG scores); Fee/Contract Payment Files (ICD9 codes, CPT codes and bed days of care); VA maintained Emerging Pathogens and Immunology Case Registries (hepatitis and HIV data); Pharmacy Benefits Management (prescription data); DSS patient specific cost data.

No	Other Federal Agency Source(s)
----	---------------------------------------

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.

No	State Agency Source(s)
----	-------------------------------

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	Local Agency Source(s)
----	-------------------------------

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	Other Source(s)
----	------------------------

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	Web Forms:	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.")

In a few instances, data can be submitted via a Secure Socket Link to the secure portion of ARC web site (<http://vawww.arc.med.va.gov/>). This site references the VA Privacy and Security site (<http://www.va.gov/privacy/>), as well as the VA Disclaimer site (<http://www.va.gov/disclaim.htm>) and the VA FOIA site (<http://vawww.va.gov/OIT/CIO/FOIA/default.asp>). As noted earlier, the ARC site exists within the VA firewall and is not accessible outside of the VA Enterprise Solution WAN.

No	Paper Forms:	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.

No	Electronic File Transfer:	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	Computer Transfer Device:	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.

Data is extracted from the VHA sources mentioned above and transferred over the secure VHA WAN via FTP.

No	Telephone Contact:	Information is collected via telephone.
----	---------------------------	---

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

Yes	Other Collection Method:	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.

Although the collection of data via CD is unlikely, the possibility that this method of data could be used exists.

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?

No

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

5.4.b) Is the data collection mandatory or 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?

5.4.d) Is the data collection new or 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.)

<input type="checkbox"/>	Not applicable
<input type="checkbox"/>	Privacy notice is provided on each page of the application.
<input type="checkbox"/>	A link to the VA Website Privacy Policy is provided.
<input type="checkbox"/>	Proximity and Timing: the notice is provided at the time and point of data collection.
<input type="checkbox"/>	Purpose: notice describes the principal purpose(s) for which the information will be used.

	Authority: notice specifies the legal authority that allows the information to be collected.
	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.
	Disclosures: 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:

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

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 ARC does not obtained data directly from individuals. All of the data comes from other VA Files and Databases.

No	Paper Forms:
----	---------------------

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.

No	Electronic File Transfer:
----	----------------------------------

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	Computer Transfer Device:
-----	----------------------------------

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?

The ARC does not obtained data directly from individuals. All of the data comes from other VA Files and Databases.

No	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.

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.

The ARC does not obtained data directly from individuals. All of the data comes from other VA Files and Databases.

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.

	Paper 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.

	Electronic File Transfer:
--	----------------------------------

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.

	Computer Transfer Device:
--	----------------------------------

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.

	Telephone Contact Media:
--	---------------------------------

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.

	Other Media
--	--------------------

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:

Inquires/extracts from the Austin databases are specific in nature and limited in scope.

5.6.b) How is data checked for completeness?

Aside from the technical tools used to ensure data transfer accuracy, a comprehensive data validation program has been implemented at the ARC. Subsequent to ARC processing, data is validated against the original data sources to ensure consistency. In addition, the ARC takes advantage of various third party data sources such as the VA Support Service Center (VSSC) to validate results. The ARC also conducts internal table/field level validation processes such as comparing bottom line and/or station/VISN level information. A process is also in place for overall validation of VERA results. Naturally, field (i.e. station level reviews) reviews are conducted to ensure accuracy and integrity of data at a lower level of granularity.

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

The ARC is notified of the status of approved Austin data as soon as it is available. Austin files are date specific by convention. In addition to prior timeframe comparisons (month to month, quarter to quarter, year to year and bottom line comparisons), validation is conducted at detailed levels both within the ARC and at other levels within VHA to ensure consistency.

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

As noted earlier, inquires/extracts from the Austin databases are specific in nature and limited in scope; only relevant data is extracted. Also, as noted above, in addition to prior timeframe comparisons (month to month, quarter to quarter, year to year and bottom line comparisons), validation is conducted at detailed levels both within the ARC and at other levels within VHA to ensure consistency.

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

PIA SECTIONS 6 - 13

Project Name

Allocation Resource Center(ARC)-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	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.

The contractor with access to ARC data fill a data analysts role. His services are acquired via GSA contract GS07T00BGD0063. He has limited access to records within the database.

All IT contracts are required to be reviewed by the ARC ISOs. 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 VA's Office of Cyber and Information Security (OCIS) on an annual basis.

Contract employees are hired through GSA sanctioned human resource providers, and familiarization with and knowledge of the Privacy Act of 1974 is a required part of the contract. Contracts include specific security and confidentiality requirements as required by policy. In addition, contractors with access to the database are required to complete IT security training and sign a rules of behavior statement, which addresses sanctions for non-compliance. Comprehensive audit trails exist for access to sensitive data.

No	Internal Sharing: Veteran Organization
----	---

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.

No	Other Veteran Organization
----	-----------------------------------

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.

No	Other Federal Government Agency
----	--

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.

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.

--	--

Yes	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.

Workload and cost information is used by staff throughout VHA.

--	--

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

For the purpose of data analysis, approved users within the VHA community. These users are endorsed by their local facility directors as having a need to know the information as part of their official duties. Users that have access to the information in the system fulfill a data analyst role.

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

Via signed security access agreements and confidentiality statements. A facility director will endorse an applicant for access. Job position is reviewed to determine what data is required to fulfill job functions, access to data is granted based on need-to-know and job function

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

Yes, as stated in the security and confidentiality agreements, as well as the ARC Security Plan. This information is further enforced via mandatory annual training, performance plans and performance descriptions.

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

Access is restricted, primarily via secure report options. Raw data is only available to approved individuals at the ARC.

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)

The ARC tracks user activity through the creation of audit trails (including the specific user as well as the data accessed) and provides the following notification to prior to accessing secure information: "Please be aware that the ARC collects time stamped personally identifiable information (user name and IP address) when confidential data is extracted from our secure interactive pages." Users are reminded that all access or use of the system constitutes an understanding and acceptance of the terms listed in the "ARC Access Agreement" and are provided an opportunity to review the agreement prior to accessing data. Users are provided contact information to report any problems. The system terms of use are also made available prior to accessing sensitive data and include, among other things, the need for confidentiality, official use requirements, and misuse ramifications. Annual reviews are conducted for each user. Program (station, VISN and so forth) Directors verify continued need for access to sensitive data and certify that the individual meets the security criteria in use at each facility pertaining to the handling of sensitive information. Directors acknowledge their responsibility to notify the ARC whenever changes in access are necessary such as separation, reassignment or abuse of access privileges. They certify that the sponsored individual is aware that misuse of sensitive information, and/or government owned computer systems may be punishable by fines, or imprisonment. Annual privacy and security training are OCIS

requirements and address concerns related to the ARC site. Direct access by ARC staff to the database is tracked at the system level. ARC users are informed that the system will be monitored and that only official access is permissible. System access logs are created at the operating and application (Oracle) levels. IT Security is addressed both at the enterprise and program levels, with funding for both efforts being provided by individual program offices. At the Department level, the CIO's Office of Cyber and Information Security (OCIS) 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 OMB and NIST. This guidance is contained in VA Directive 6210, Automated Information Systems Security. Overarching mission strategies of this directive, as well as a structured framework for effective implementation of programmatic goals, are articulated the VA IT Security Program Management Plan, which is updated quarterly. Additionally, OCIS globally manages the implementation of enterprise-wide cyber security solutions that include intrusion detection, anti-virus protection, authentication, independent vulnerability scanning and penetration testing, a centralized incident response mechanism, as well as security awareness and role-specific training. OCIS also provides a risk management project office that assists management, technical, and security personnel with conducting risk assessments based on business case. This structure achieves economies of scale through providing a central management focal point for Department-wide IT security activities, as well as ensures that a strong security baseline is effectively integrated into VA's emerging enterprise architecture. At the program level, IT security is provided through CFO funding. The ARC maintains a comprehensive security program. The ARC security plan in place is dated January 30, 2007; a contingency plan is also in place dated February 12, 2007. The ARC has a current Full Authority to Operate (FATO). Staff privacy and security training is conducted annually. The security program was reviewed and approved by VHA CIO. Database security is accomplished via Oracle security products. As suggested above, the technology refreshment will permit the ARC to implement the latest Oracle applications. It includes licensing for Oracle's Advanced Security application. This product received Common Criteria certification through an evaluation program run by the National Security Agency and the National Institute of Standards and Technology. It received Common Criteria Evaluation Assurance Level Four. It is eligible for use in systems that handle sensitive information, including data concerning national security. The ARC estimates that approximately \$170,000 will be devoted to security in FY09 for issues such as Information Security Liaison activities, staff training/travel, recurring support costs (e.g. Oracle's Advanced Security option, SSL and so forth).

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)

No

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.

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

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

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.

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

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.)

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.)

	The application will provide a link that leads to their information.
	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
	The application will provide a phone number of a VA representative who will provide instructions.
Yes	The application will use other method (explain below).
	The application is exempt from needing to provide access.

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

The ARC is a secondary user of VHA business data in the National Patient Databases-VA (121VA19) systems of records. The data can only be modified at its source.

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

The ARC is a secondary user of VHA business data in the National Patient Databases-VA (121VA19) systems of records. The data can only be modified at its source.

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

The ARC is a secondary user of VHA business data in the National Patient Databases-VA (121VA19) systems of records. The data can only be modified at its source.

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

The ARC is a secondary user of VHA business data contained in the National Patient Databases-VA (121VA19) system of records. The data can only be modified at its source.

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

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

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](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.

The data maintained in the "National Patient Databases-VA" (121VA19) will be retained in accordance with the system of records notice. Trending and analysis information will be retained for 10 years.

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

Data is physically destroyed or eliminate in accordance with government material management standards.

7.c) Where are procedures documented?

Procedures are documented in the ARC Information Security Plan and are periodically reviewed to ensure applicability and compliance with appropriate guidelines.

7.d) How are data retention procedures enforced?

Data retention procedures are enforced by the local ISO and DBA.

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

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

The ARC is a secondary user of data managed within other systems. This question does not apply to the ARC.

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:

In addition to Security and Contingency Plan reviews, periodic Risk Assessments and Security Controls Assessments are conducted in accordance with OCIS guidelines.

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.

<ul style="list-style-type: none"> • A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.
<ul style="list-style-type: none"> • A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).
<ul style="list-style-type: none"> • 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"> • 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?
<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>OCIS globally manages the implementation of enterprise-wide cyber security solutions that include intrusion detection, anti-virus protection, authentication, independent vulnerability scanning and penetration testing, a centralized incident response mechanism, as well as security awareness and role-specific training. OCIS also provides a risk management project office that assists management, technical, and security personnel with conducting risk assessments based on business case. This structure achieves economies of scale through providing a central management focal point for Department-wide IT security activities, as well as ensures that a strong security baseline is effectively integrated into VA's emerging enterprise architecture. At the program level, IT security is provided through CFO funding. The ARC maintains a comprehensive security program. The ARC security plan in place is dated January 30, 2007; a contingency plan is also in place dated February 12, 2007. The ARC has a current Full Authority to Operate (FATO). Staff privacy and security training is conducted annually. The security program was reviewed and approved by VHA CIO. Database security is accomplished via Oracle security products. As suggested above, the technology refreshment will permit the ARC to implement the latest Oracle applications. It includes licensing for Oracle's Advanced Security application. This product received Common Criteria certification through an evaluation program run by the National Security Agency and the National Institute of Standards and Technology. It received Common Criteria Evaluation Assurance Level Four. It is eligible for use in systems that handle sensitive information, including data concerning national security. The ARC estimates that approximately \$170,000 will be devoted to security in FY09 for issues such as Information Security Liaison activities, staff training/travel, recurring support costs (e.g. Oracle's Advanced Security option, SSL and so forth).</p>
<p>8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.</p>
<p>IT Security is addressed both at the enterprise and program levels, with funding for both efforts being provided by individual program offices. At the Department level, the CIO's Office of Cyber and Information Security (OCIS) 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 OMB and NIST. This guidance is contained in VA Directive 6210, Automated Information Systems Security. Overarching mission strategies of this directive, as well as a structured framework for effective implementation of programmatic goals, are articulated the VA IT Security Program Management Plan, which is updated quarterly.</p>

<p>9. CHANGE RECORD</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"> • 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.
<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"> • 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.
<p>New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic</p>

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.

No changes were made to ARC systems as a result of completing this PIA.

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 assessment⁹. 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)

Dave Pike 5-31-07 (updates since 6-2-05).

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