

Privacy Impact Assessment - 2009 (Form) / Pharmacy Re-Engineering and IT Support-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:

Pharmacy Re-Engineering and IT Support-2009

1.1.b) OMB Unique Project Identifier:

029-00-01-11-01-1184-00-110-248

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.

Pharmacy Re-Engineering and IT Support is undergoing modernization as defined by the HealtheVet - VistA strategy. The Project scope is to replace current pharmacy software modules with new technology by re-engineering, new development and purchase of commercial products. In addition, this initiative aligns with the Services for Citizens category under the federal Business Reference Model, with a particular focus on the Health subcategory. This project will facilitate improved VA pharmacy operations, customer service and patient safety, concurrent with pursuit of full re-engineering of VA pharmacy applications to support a new patient centric business model. It will address critical needs, such as the following benefits for the veteran: improved patient safety by 50% reduction of Adverse Drug Events and saving approximately 115 lives for serious errors, increased access to benefits by improving formulary management support and improved fiscal performance by reducing 5% in cost of inventory. Systems limitations and inconsistent pharmacy processes have hindered the VA's ability to provide efficient pharmacy service. The re-engineered pharmacy system will address these inefficiencies and enhance pharmacy data exchange, as well as clinical documentation capabilities, in an integrated fashion that will improve operating efficiency. It will provide a flexible technical environment to adjust to and meet future business conditions and needs in the clinical environment, an environment that is focused on the patient with robust decision support safety features. However, the implementation of the Pharmacy Re-Engineering project is dependent upon the personnel and budgetary resources and the HealtheVet strategy and deployment schedule. The Pharmacy re-engineered system will fit into the One VA architecture by implementing the standards proposed by the Consolidated Health Informatics group. The re-engineered system will also utilize enterprise level services such as Enterprise Level Authentication and Authorization Service, Clinical Data Service to access Health Data Repository, Person Service to identify patients and access patient demographics, Standard Data service to access standard enterprise level reference tables, Enterprise Terminology service to access standard clinical code sets, Ordering Service to handle lab orders and Infrastructure services such as a common delivery service, auditing service, defect logging service etc.

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:	Michele Davis
Organization:	Health Provider Systems
Telephone Number:	727-319-1311
Email Address:	Michele.davis@med.va.gov
1.2.b) Project Manager:	
Title:	Michael L. Mims, Sr. Project Manager

Organization:	Health Provider Systems
Telephone Number:	205-554-3452
Email Address:	mike.mims@va.gov
1.2.c) Staff Contact Person:	
Title:	Michele Davis
Organization:	Health Provider Systems
Telephone Number:	727-319-1311
Email Address:	Michele.davis@med.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.)

The Pharmacy application does not store PII, but obtains it for display and identify verification from other Vista Applications.

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.

Knowledge of the patients' healthcare while being served by the DoD medical systems is critical to improve the effectiveness of care and safety of that patient when he is under the care of the VA. The ability to share this information between the VA and DoD systems in a secure fashion will improve the ability of the VA to care for these patients by providing appropriate access to the patient's medical history from their military service along with information on the care received from VA facilities. This data will be used to ensure correct identification of the patient and their medical records, as well as in the performance of billing activities as appropriate under VA regulations.

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

The Pharmacy will adhere to HIPPA standards mandated by Congress.
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.
More than 20,000,000
3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.
(2) Development/Implementation
3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.
The Pharmacy system will be deployed as an iterative process with version.5 in March 2008 with the final version 5.0 being deployed in december 2014.
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),
24VA19 - Patient Medical Record replaces 24VA136
(2) The name of the System of Records, and
Patient Medical Records
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
http://vawww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf
<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.
It was created for the VA Vista Application.
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.

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

Explanation:

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

PIA SECTION 5

Project Name

Pharmacy Re-Engineering and IT Support-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.

The primary use of the clinical data collected is to provide healthcare services to our veterans. The information is used to provide improved and easier access to medical knowledge, expertise and care, and improve the quality of life and economic status of veterans. Demographic information such as name, social security number, date of birth, sex, and race will be used to correctly identify the patient to ensure clinical data is matched to the correct patient record both for clinical purposes and to support billing activities as appropriate for the patient. Name and address will be used to contact the patient via postal mail. Statistical information will be derived from this clinical data and used to support research and study initiatives.

Yes	Other Personal Information of the Veteran or Primary Subject
-----	---

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

Personal Insurance Information for 3rd party billing. The following fields: BIN, PCN# and the Unique Insurance Identifier # are encapsulated and transmitted to WEB MD and the adjudicating 3rd Party Insurance.

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

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

No	Service Information
----	----------------------------

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

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

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

The ICD9 code that captures allergies will be used to communicate and provide health information for the patient.

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.

No	Rehabilitation Information
----	-----------------------------------

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

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.

The primary use of the clinical data collected is to provide healthcare services to our veterans. The information is used to provide improved and easier access to medical knowledge, expertise and care, and improve the quality of life and economic status of veterans. Demographic information such as name, social security number, date of birth, sex, and race will be used to correctly identify the patient to ensure clinical data is matched to the correct patient record both for clinical purposes and to support billing activities as appropriate for the patient. Name and address will be used to contact the patient via postal mail. Statistical information will be derived from this clinical data and used to support research and study initiatives.

The system also collects next of kin contact information for emergency contact purposes.

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

Veteran Source

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

This includes data provided by the veteran including demographic information such as DOB and SSN as well as clinical information such as allergies and medical 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.

Relevant VA database containing patient identity information (for example, HDR and CPRS) will be accessed by the Pharmacy System.

Yes	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.

Department of Defense. Knowledge of the patients' healthcare while being served by the DoD medical systems is critical to improve the effectiveness of care and safety of that patient when he is under the care of VA. The ability to share this information between the VA and DoD systems in a secure fashion will improve the ability of VA to care for these patients by providing appropriate access to the patient's medical history from their military service along with information on the care received from VA facilities. This data will be used to ensure correct identification of the patient and their medical records, as well as in the performance of billing activities as appropriate under VA regulations.

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.")

System is still in the design phase and will use web forms media upon implementation.

Yes	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.

The pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

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.)

No	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.

Yes	Telephone Contact:	Information is collected via telephone.
-----	---------------------------	---

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

The pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

No	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.

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?

Mandatory

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?

Persons presenting for care are notified of the Privacy Policy and of the mandatory nature of the data collection. The Notice of Privacy Policy is mailed to each veteran upon enrollment.

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	Not applicable
Yes	Privacy notice is provided on each page of the application.
Yes	A link to the VA Website Privacy Policy is provided.

Yes	Proximity and Timing: the notice is provided at the time and point of data collection.
Yes	Purpose: notice describes the principal purpose(s) for which the information will be used.
Yes	Authority: notice specifies the legal authority that allows the information to be collected.
Yes	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.
Yes	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:

These guidelines stated in 5.4.e.1 will be adhered to.

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 pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

Yes	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.

The pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

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?

No	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 pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

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.

The pharmacy application conducted a business process analysis in 2005 which identified the business needs. A deployment plan has been developed to support a phased approach. The first release will occur in 2008 with the complete system to be deployed in 2011. For the final deployed Pharmacy system, web sites, paper forms, and telephone processes will be utilized, but have not been designed or implemented at the current time. The URL's, form numbers, etc are yet to be determined.

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.

	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:

The Pharmacy application completed the business process analysis phase in 2005 which identified the business needs. As per this analysis, required data elements will be incorporated into data collection forms under the caveat that only the minimum data needed to accomplish the function of this service will be collected.

5.6.b) How is data checked for completeness?

Data collection forms will be checked for completeness before being accepted. Users will be required to complete data collection forms fully.

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

Time sensitive data will be time stamped to allow appropriate disposition. It is anticipated that no time sensitive data will be reviewed with individuals to ensure timeliness.

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

This system will interface with common services for patient selection and other functions. It is anticipated that data entered by users will be authenticated prior to being saved.

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

PIA SECTIONS 6 - 13

Project Name

Pharmacy Re-Engineering and IT Support-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.

In support of the system development these are the following contractors and their respective number; EDS 776-E70032, SWRI V776P-0409 and CACI 776-E70044.

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.

Yes	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.

The following data will be shared with the Department of Defense healthcare system: Patient and Outpatient medication, and demographic information. Data sharing is required for the purpose of performing order checking and to identify the right patient.

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.

Yes	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.

VA Health Data Repository: Medication Order data. It is central repository for the VA. CPRS will be receiving Patient Order information from pharmacy until HDR is able to provide the data. CPRS is the primary ordering engine for the VA. The pharmacy data will be provided to CPRS for display and to allow actions to be taken on those orders. The VHA security group is responsible for protecting the privacy rights of patient's data.

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.

Pharmacy information may be provided to outside health care providers in order to treat patients through printing copies of the information in the Pharmacy Re-engineering system.

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

This system has just completed the business process analysis phase so no personal information is yet stored. It is anticipated that users will have access only to the minimum necessary standard. VA and DOD have a sharing agreement in order to share PHI (personal health information).

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

The pharmacy system will interface with enterprise wide authentication authorization and access to be implemented by the OSCI in calendar year 2006. Authenticated users will be assigned roles based access.

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

The data will be shared with the Department of Defense healthcare system as specified in our sharing agreement (Interagency Sharing Agreement) with that organization. Future plans include expanding these sharing agreements to include Indian Health Service. No other agencies have been identified for sharing of this data at this stage of the project.

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

User access will be restricted to the minimum necessary to perform their assigned 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)

All users will participate in the annual VHA Privacy Policy Training.

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.

Information is password protected and compliant with HIPAA Security standards. When information is disclosed it is done so only in accordance with legal authorities in all applicable Federal privacy laws and regulation. Information disclosed electronically is always encrypted.

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

HealthVet Vista for internal data sharing and when sharing data externally the recipients of the data are required to appropriately protect it while in their IT systems . For example, DOD will be responsible for securing data received from the system.

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

Pharmacy will employ authentication procedures when information is transmitted electronically. Information from the system may also be disclosed in a paper format pursuant to appropriate legal authority under all applicable Federal privacy laws and regulations.

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.

Yes.

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

The recipients of shared information are required to adhere to the HIPPA requirements.

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

For direct electronic access into VHA systems, privacy and security training as required in policy. For access via paper, no training is required as this is considered a disclosure pursuant to appropriate legal authorities.

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.)

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

Individuals must submit a written request to the VHA health care facility where they receive care requesting copies of their own information. VA Form 10-5345a may be utilized to meet the written request requirements. Once the request is received the Release of Information unit will process the request in accordance with VHA Handbook 1605.1.

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

Individuals must submit a written request to the VHA health care facility where they receive care requesting an amendment to their information. Once the request is received the facility Privacy Officer will be process the request in accordance with VHA Handbook 1605.1. If the amendment request is denied, the individual will be given their appeal rights to the Office of General Counsel.

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

If the individual appeals the amendment request and it is denied, he may submit a Statement of Disagreement to be filed in the record.

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

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

7 Retention and Disposal

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

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

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

System of Records Notices may be accessed via:

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

or

http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html

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>

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

Paper documents at health care facilities related to authorizing the fee basis care and the services authorized, billed and paid are retained at the facility for a minimum period of three years after the last episode of care. Following the three-year retention period these paper records are transferred to a records facility for seventy-two (72) more years of storage. Automated storage media and other paper documents that are included in this system are retained and disposed of in accordance with disposition authorization approved by the Archivist of the United States.

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

Paper documents may be shredded or burned, and record destruction documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG 025 Version-2/VA Policy. If a degausser is not available, the media is destroyed by smelting, pulverization or disintegration. 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 accessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

7.c) Where are procedures documented?

The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. 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.

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 (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

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.)

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:

The system has just completed the business process analysis phase. It is anticipated that the application will provide the ability for individuals to view instructions as indicated above.

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

Yes

8.2 Project-Specific Security Measures

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

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

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

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

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

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

The data will be protected by implementing the minimum baseline security controls identified in NIST SP 800-53 based on the FIPS 199 system categorization. All of the security requirements described in federal law have been captured and are being maintained in the HealthVet-VistA requirements repository, and are used by application developers to ensure compliance with all current policies, standards, and legislation. In addition, a security plan is in place for the Pharmacy Re-engineering investment, and contingency plans and configuration management plans are being developed in accordance with NIST standards. An established process for granting and terminating user access to VHA systems is in

place to ensure that access to VHA data and systems is controlled, access is limited to an individual's role and based on a need to know, and is terminated or revised when a person no longer requires access or changes positions. The procedure includes approval by the information system owner for access to options, menus, and security keys. Users are also required to undergo background screening appropriate for the position, complete orientation and annual awareness training in security and privacy topics, and sign a Rules of Behavior form initially and annually. VA has adopted the strengthened password policy that was developed by the Federal CIO Council. VHA is also the covered entity for HIPAA purposes, and has taken a number of actions to ensure compliance with the HIPAA security rule including appointment of HIPAA Implementation Team members across VHA facilities, self-assessment tools for individual sites to determine levels of compliance and vulnerability areas/areas for improvement, and established a plan of action and milestones for the required security controls so that implementation and ongoing compliance can be monitored at the Department level.

The Department's Office of Cyber and Information Security (OCIS) operates VA's Security Operations Center (SOC), which is responsible for providing a centralized incident response and recovery mechanism, as well as other global security services such as penetration testing, vulnerability scanning/assessments, firewall management, intrusion detection and prevention monitoring with event correlation, forensics analysis, malicious code/threat analysis and associated security architecture device management. The SOC also manages the current Public Key Encryption (PKI) "soft certificates/key" infrastructure. Additionally, as part of the Department-wide Security Program, the CIO has established a centralized mechanism to issue minimum configuration management standards; oversee patch management (including testing and deployment); deploy the security architecture such as network and host-based intrusion prevention, anti-spyware and anti-spam solutions; and enhance the existing Department-wide anti-virus program. Under the general oversight of the CIO, the Office of Human Resources is in the process of establishing the capability for interfacing physical access and logical access controls (including Public Key Infrastructure, "hard certificates/key") through a single Personal Identity Verification (PIV) card, which will take the place of existing access badges for entry into VA facilities.

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

The Department follows FIPS and NIST standards and guidelines in addressing security requirements through the system security life cycle. The process begins with a security categorization of the system in accordance with FIPS 199 and NIST SP 800-60, and minimum security controls are selected using NIST 800-53 and FIPS 200. Risk assessments are conducted on the investments in accordance with NIST SP 800-30, and security controls adjusted accordingly. The system security plans are developed using NIST SP 800-18. Security controls are assessed for correct implementation, intended operation, and meeting security requirements following NIST SP 800-53A and SP 800-26. NIST SP 800-37 is followed for all Department authority to operate decisions for authorizing information system processing. System owners establish continuous monitoring processes to track changes to the information systems that impact security controls and assess security control effectiveness on an annual basis. The Department operates a plan of action and milestone (POA&M) database to monitor and track remediation of vulnerabilities identified during security controls assessment testing, to monitor compliance with HIPAA security rule, and to monitor and track recommendations made by oversight groups such as the Office of Inspector General for improvements to VHA's information security programs.

9. CHANGE RECORD

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

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

No

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

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

No

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

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

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

11. PIA CONSIDERATIONS

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

The Pharmacy application completed the business process analysis phase in 2005 which identified the business needs. As per this analysis, required data elements will be incorporated into data collection forms with the contingency that all choices, methods, and controls remain consistent with this information contained within the 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)

Michael Mims/Jeff Ramirez May 18, 2007

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