

Privacy Impact Assessment - 2009 (Form) / Health Data Repository-2009 (Item)

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

Health Data Repository-2009

1.1.b) OMB Unique Project Identifier:

029-00-01-11-01-1183-00-110-248

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.

The HDR is a repository of clinical information normally residing on one or more independent platforms for use by clinicians and other personnel in support of veteran-centric care. The data are derived from legacy, transaction-oriented systems and organized in a format to support clinical decision-making in support of health care, independent of the physical location of patient information. The HDR will hold individual patient medical records that delineate all aspects of a veteran's clinical care across the continuum within the VHA. Storage and retrieval of data from Veterans Health Information Systems and Technology Architecture (VistA) to the repository is in real-time to accommodate clinical needs to care for the patients. The repository is intended to be the equivalent of the legal medical record. The HDR would provide complete, up-to-date online patient data to healthcare providers anywhere in the system at the point of care. Therefore, this would increase clinician productivity, facilitate medical decision-making, and improve quality of care. Providing near-real time, comprehensive, longitudinal, treatment data to clinicians would also enhance patient safety. The benefits of this feature cannot be underestimated in light of its impact on patient safety. It will provide common access to accurate, consistent, and reliable information across clinical/business lines in VHA, thus reducing the likelihood of clinical error. VHA Information Technology Architecture (ITA) group has recognized the need for the repository for the last seven years. This project aligns with the VHA IT Architecture goal to support access to, and portability of information throughout VHA. Without a HDR, sharing data between sites would not be possible, which could compromise patient care. The repository will allow access to clinical patient information regardless of VHA location, allow other medical agencies to share information with VHA, provide improved health care through decision support tools and alerts of required actions, provide the components for the requirements of the legal record of patient care and eliminate the need for paper documents, provide an environment for population based reporting, provide improved information security, enable enhanced patient safety, convenience, high quality care and measurable health care delivery, maintain data quality, confidentiality, availability and integrity to ensure patient safety and protect veteran privacy.

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:	Greene, Matthew
Organization:	HSD&D
Telephone Number:	801-588-5228
Email Address:	Matthew.Greene2@va.gov

1.2.b) Project Manager:	
Title:	Smith, Gloria
Organization:	HSD&D
Telephone Number:	801-588-5052
Email Address:	gloria.smith@va.gov
1.2.c) Staff Contact Person:	
Title:	Andrews, Tiffany
Organization:	HSD&D
Telephone Number:	540-850-4364
Email Address:	tiffany.andrews@va.gov

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

2. DETERMINATION OF PIA REQUIREMENTS:

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

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

Yes

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

No

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

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

Part II. Privacy Impact Assessment

3. PROJECT DESCRIPTION:

Enter the information requested to describe the project.

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

The Health Data Repository is defined as a repository of clinical information normally residing on one or more independent platforms for use by clinicians and other personnel in support of longitudinal patient-centric care. Data will be organized in a format that supports the clinical decision-making process requisite to patient care, independent of the physical location of that patient information.

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

Title 38 United States Code Section 501(b) and Section 304
3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.
1,000,000 - 9,999,999
3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.
(2) Development/Implementation
3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.
09/30/2009 HDR-IMS: 9/29/06 HDR II: · National: 9/28/07 · Regional: 9/30/09 HDR Data Warehouse: 9/29/06
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 121VA19
(2) The name of the System of Records, and
24VA19 : Patient Medical Records - VA 121VA19 - National Patient Databases - VA
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
18428 Federal Register / Vol. 69, No. 67 / Wednesday, April 7, 2004 / Notices 24VA19: http://vawww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf
18436 Federal Register / Vol. 69, No. 67 / Wednesday, April 7, 2004 / Notices 121VA19 : http://vawww.vhaco.va.gov/privacy/Update_SOR/SOR121VA19.pdf
IMPORTANT: For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.
4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?
Yes
4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?
Created for another project or system

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

A Systems of Records (SOR) already exists that provides for Routine Uses that gives authority to disclose without getting an authorization from the individual. Since an SOR is already in place, an SOR specific for the HDR project is not required.

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

Health Data Repository-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.

A limited amount of personal information will be collected to allow unique patient identification in the HDR. These data elements include:

Name, Sex, Date of birth, Marital status, Race, Ethnicity, Religious preference, Social Security Number, Address, Phone number – residence and work

Mother's maiden name, Date of death, Integration control number.

No

Other Personal Information of the Veteran or Primary Subject

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

Yes	Dependent Information
-----	------------------------------

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

Categories of individuals covered include the spouse, surviving spouse, and children of veterans who have applied for health care services under Title 38, United States Code, Chapter 17. Minimal dependent information will be collected in the HDR. This will be limited to dependent information included in text-based documents where the role of caregivers or family histories is considered important to the treatment of the patient.

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

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

Minimal service information will be collected in the HDR. This will be limited to service information included in text-based documents where the veterans' military history is considered important to the treatment of the patient. This may include information on areas where they served, exposure to agent orange or radiation, service-connected conditions, combat experience, etc. Some of this information will also be included in compensation and pensions examination reports.

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

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

The HDR will store medical information collected on veterans. The clinical domains include:

Allergies/Adverse Reactions; Audiology & Speech Pathology; Clinical Decision Support; Clinical Procedures and Medicine; Compensation and Pension Exams; Consultations; Demographics (see above); Dental; Encounters; Event Capture; Health Factors; Home-Based Primary Care; Immunizations/Skin Tests; Laboratory; Mental Health; Nursing; Nutrition and Food Service; Orders; Patient Education; Pharmacy; Problems; Prosthetics; Radiology; Resident Assessment Instrument/Minimum Data Set; Registries; Surgery; Text Documents; Visual Impairment/Blind Rehab; Vitals; Women's Health.

This information will be used for clinical decision-making, enhanced patient safety, research studies, population-based reports, biosurveillance, disease outbreaks, and continuity of care with other healthcare providers veterans may utilize (i.e., Department of Defense, community physicians, specialty laboratories).

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.

--	--

Yes	Education Information
-----	------------------------------

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

Patient educational information will be collected and made available to clinicians when treating these patients. This will help veterans and their caregivers understand their medical conditions and alert them to signs and symptoms that may require future treatment.

--	--

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

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

Rehabilitation information will be collected from veterans being treated in special programs. Rehabilitation programs are established to treat veterans who have suffered certain injuries and conditions. Injuries and conditions that qualify include head injuries, spinal cord injuries, strokes, cardiac conditions, blindness, post traumatic stress disorders, alcohol and drugs, amputees, etc. Functional independence and outcomes measurements will also be collected.

--	--

No	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.

--	--

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.

Veterans and their caregivers are currently able to enter vital measurements and blood glucose levels into Home Telehealth devices. The Home Telehealth system sends this data to the local VistA system where the veteran is primarily treated. This data is then stored in the HDR-IMS repository.

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.

VA files and databases, specifically the VistA system files, will be the primary source of patient data in the HDR. HDR is collecting data from each local VistA database (128). HDR-Hx is currently extracting selected legacy data from the Vitals, Outpatient Pharmacy, Allergies, and Demographic files up to a specified date. Then, HDR-IMS takes over and collects the same data in real-time from the local databases via HL7 messaging transmissions. The data collected from both the Hx and IMS repositories is then inserted into the HDR Data Warehouse to be used for research and population-based studies. The HDR II, currently in design, will collect veteran information from both VistA files and re-engineered packages from all thirty (30) domains. This data will be used for clinical decision-making, enhancing patient safety, research studies, population-based reports, biosurveillance, disease outbreaks, and continuity of care with other healthcare providers veterans may utilize (i.e., Department of Defense, community physicians, specialty laboratories).

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.

Clinical data from the Department of Defense's Clinical Data Repository (CDR) is being shared and stored in the HDR on patients discharged from the military through the CHDR project (DoD Clinical/VA Health Data Repository). This includes patients primarily treated by the VA after discharge or those veterans eligible to be dual consumers of both VA and DoD medical facilities. This currently includes only demographics, outpatient pharmacy and allergies information. Additional data will be shared in the future, but those domains haven't identified yet. This data will be used for patient treatment and clinical decision-making.

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.

No	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.")

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.

Yes	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.)

Veterans and their caregivers are currently able to enter vital measurements and blood glucose levels into Home Telehealth devices. The Home Telehealth system sends this data to the local VistA system where the veteran is primarily treated. This data is then stored in the HDR-IMS repository.
HDR also
Most of the patient information stored in the Health Data Repository will be extracted from the VistA databases through an electronic data extraction mechanism. In the future, the HDR will collect patient information electronically via HL7 messages and other means.

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.

Current information collected in the Health Data Repository is either being extracted directly from the VistA databases (HDR-Hx) or being transmitted via HL7 electronic transmissions (HDR-IMS).

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

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

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?

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.
<input type="checkbox"/>	Authority: notice specifies the legal authority that allows the information to be collected.
<input type="checkbox"/>	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.
<input type="checkbox"/>	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.

No	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.

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.

Yes	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?

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.

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."

Yes

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

Secondary uses of patient information are specified in the Privacy Act of 1974; System of Records 24VA19 Patient Medical Records - VA. All potential secondary uses of HDR data are covered by the routine uses of records maintained in this system of records.

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.

No	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.

No	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.

Yes	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.

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 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.

Current information collected in the Health Data Repository is either being extracted directly from the VistA databases (HDR-Hx) or being transmitted via HL7 electronic transmissions (HDR-IMS).

No	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.

No

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 HDR Data Content Team in collaboration with the appropriate stakeholders and subject matter experts have identified all required data elements that will reside in the HDR. This will be the only data collected in the HDR.

5.6.b) How is data checked for completeness?

The HDR Software Quality Assurance (SQA) team conducts data quality analyses of statistically significant samples for each of the clinical domains stored in HDR-Hx. The business owners own the data quality issues however.

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

Current data is sent to HDR IMS by a continuous feed as it is generated from the sites. The HDR sends acknowledgements that all data was received. Updates and corrections are also generated from the sites and update data stored in HDR. HDR-Hx extracts historical/legacy data from local sites that is not intended to be current. The HDR Data Warehouse receives data from Hx and IMS by a nightly feed and is updated daily.

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

During the testing process, data is generated in the legacy system. The transactions are reviewed, ensuring that the data store and any subsequent data updates are correct. Test cases are created and executed for each clinical domain – data store, data updates, data retrieval, patient merges and patient correlation with the MPI. Client applications and projects such as CPRS Remote Data Views (RDV), Remote Data Interoperability (RDI), Vista Web (VW), Clinical/Health Data Repository (CHDR) and Data Warehousing also provide another level of data validation as data is stored and retrieved.

In production, face validity of data will be accomplished by clinicians, code fixes will be rapidly deployed to the database following a robust configuration management environment.

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

PIA SECTIONS 6 - 13

Project Name

Health Data Repository-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
-----	---------------------

No	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.

All IT contracts are required to be reviewed at the system level by ISOs and at the enterprise level by OCIS to ensure that security requirements are addressed. Contract language is written to require positive background checks, complete mandated training, and comply with VA security policies and procedures for protecting VA's systems and data. Contractors must also follow the VHA IT security rules, which include signing rules of behavior and nondisclosure agreements, and completing annual awareness and privacy training modules. This is monitored and verified as part of FISMA compliance reporting. Compliance with the mandated security and privacy training requirements for all employees, volunteers, and contractors is reported to VA's Office of Cyber and Information Security (OCIS) on an annual basis. All contractors are required to obtain, at a minimum, an OPM National Agency Check with Written Inquiries (NACI) Background Investigation. More stringent background investigation criteria may be required, with these criteria being determined by the level of access to sensitive VA information and/or systems. After the background investigation is completed, it must be favorably adjudicated through the VA Office of Security and Law Enforcement, prior to a contractor being granted access to any VA system. Contractors must also sign system Rules of Behavior and non-disclosure agreements, as well as participate in an OCIS-sponsored web-based Security Awareness Training Module and Privacy Training Module.

The contracts currently in place are with CACI (Task Orders 192-0179 HDR and 192-0190CHDR) and EDS Task Order (192-0187 HDR and 192-0188 CHDR). Task Orders are Time and Materials against a GSA Schedule. The current task orders expire on 9-30-06 and in replacement contracts are in the procurement process with anticipated award prior to 9-30-06.

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.

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

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

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

Database administrators, developers and analysts have access to personal information during the development of the HDR. Once in production, they no longer have access.

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

The PIA identified the need to locate the HDR systems at the AAC with strict access and operation controls. Access to the

HDR data must use standard VA role based controls with audit logs to comply with Privacy Act and Privacy Rule requirements.

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

Yes:

1. Austin Automation Center (AAC) Access: VA Form 9957 "ACRS Time Sharing Request"
2. Privacy and Security Rules of Behavior (OCIS) {mandatory for all VHA employees and contractors}
3. Privacy and Security Salt Lake OI Field Office Supplemental Rules of Behavior {mandatory for all VHA employees and contractors}
4. Privacy and Security Statement of Commitment and Understanding (VHA – mandatory; Contractors – currently optional)

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

Access to the HDR data must use standard VA role based controls with audit logs to comply with Privacy Act and Privacy Rule requirements.

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)

Access to the HDR data will use standard VA role based controls and that access will have specific, limited purpose. Clinicians will view data from an extract provided to the user interface, not direct access to the database. Researchers will view data from a data cube specifically prepared from an extract from the database. No other access will be provided.

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.)

<input type="checkbox"/>	The application will provide a link that leads to their information.
<input type="checkbox"/>	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.
No	The application will use other method (explain below).
Yes	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?

N/A

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

N/A

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

NO

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

Direct access into the HDR will not be allowed. Access to records and requests for corrections will occur through the site's local systems or MyHealthVet. Changes made through the local site's system or My HealthVet will be updated in the HDR when synchronization with these other systems occurs.

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.

The HDR retention process is based upon the Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006. Data will be retained in the HDR until 3 years after last episode of care. It will then be converted to an archived system but will be retrievable if/when the patient returns for further treatment. Data in the archived system will be

retained 75 years after the veteran's last episode of care.
7.b) What are the procedures for eliminating data at the end of the retention period?
Data will be purged 75 years after the veteran's last episode of care.
7.c) Where are procedures documented?
Not documented yet. HDR is still being developed.
7.d) How are data retention procedures enforced?
Not documented yet. HDR is still being developed.
7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?
Yes
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

8 SECURITY

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

8.1 General Security Measures

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

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

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

Certification and accreditation of the HDR system was completed on 8/2005. The HDR is currently operating under the guidelines of a Full Authority to Operate (FATO), which includes the Risk Assessment, for the Hx Repository, IMS Repository and Data Warehouse. HDR II plans to receive an FATO in FY07; 9/30/07 for the national instance and 9/30/09 for the regional data processing centers and Clinical Data Services (CDS) components.

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? Is so, describe these controls.

Information stored in the HDR may be accessed only by authorized VA and contract employees, such as the HDR database administrators, developers and analysts. These employees must meet the appropriate security requirements in order to work on this project. Direct access into the HDR by patients or hospital staff will not be permitted. Web access directly into the HDR will also not be allowed. The agency is following IT security requirements and procedures required by federal law and policy. Information stored in the HDR is secured in the Austin Automation Center behind a secure firewall. As part of the Certification and Accreditation process, a Full Authority to Operate (ATO) was granted in August 2005 which includes a risk assessment, assessment of the security controls to mitigate risk and assurance that the controls are in place. HDR II is in the process of acquiring an FATO beginning in FY07. As part of the Service Level Agreement with AAC, monitoring/testing and evaluation will occur regularly. The point of contact will be Bryant Headley at the AAC. Currently, an interim ATO has been granted pending completion of the risk assessment process.

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

This is covered by the FATO and information documented above.

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 PIA identified the need to locate the HDR systems at the AAC with strict access and operation controls. Access to the HDR data must use standard VA role based controls with audit logs to comply with Privacy Act and Privacy Rule requirements. No other changes have been made with respect to choices of IT systems or collection of information since the original PIA was completed.

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:

<i>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.</i>
--

Yes

<i>13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)</i>

Marcia Insley, Portfolio Manager, Health Data Systems, March 2007

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

--