

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Data collected is set by the required fields in the VistA menus. Information is collected via the phone, web, and in person to process applications for healthcare and is limited to what is needed to complete the registration process and to provide services to our veterans.

Answer:

How is data checked for completeness?

Answer:

data elements are driven by Vista software applications whereas the exclusion of essential information will not allow VA Staff to continue with the entry process. Upon exiting several Vista software applications if any data elements are missing a notification message is generated to the user and other VA staff of the missing data elements. Vista audit reports reveal missing data elements essential to the registration

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

There are automatic reminders in place to ask veterans for update information when they come in for appointments. Staff is required to update various data elements in Vista during each patient encounter which occurs via the phone, the web, or in person.

How is new data verified for relevance, authenticity and accuracy?

Answer:

Staff is required to collect only those elements needed to complete a process. There are several verification methods generated by Vista software packages that require a second level review to assure the data is relevant, authentic, and accurate. Several processes also

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

HINQS are also used to check the validity of the data supplied by the veteran. Veterans also have the opportunity to review the data that is in their medical record and ask for corrections to the record via the amendment process.

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Information is retained according to the VA Records Control Schedule for future treatment of the patients, for research purposes, legal issues and to investigate cause/effect of agents that were used during combat, i.e., Agent Orange to determine to the long term effect on the veteran population.

Answer:

Explain why the information is needed for the indicated retention period?

The retention is set by the record control schedule and varies according the documents.

Answer:

What are the procedures for eliminating data at the end of the retention period?

Answer:

Final Version
of Patient
Medical
Record is
destroyed/de-
leted 75
years after
the last
episode of
patient care
as instructed
in VA
Records
Control
Schedule 10-
1, Item
XLIII, 2.b.
(Page 190).
At the
present time,
VistA
Imaging
retains all
images. VHA
is performing
a study to
explore
whether
some images
can be
eliminated on
an earlier
schedule.
Researchers
are
responsible
for
destroying

Where are these procedures documented?

Answer:

VA Handbook
6300 and
Record
Control
Schedule 10-1

How are data retention procedures enforced?

Answer:

Field records
officers are
responsible
for records
management
activities at
their
facilities.

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.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

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.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: <http://vawww.privacy.va.gov/PIA.asp>

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and

systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name: Region 4>VHA>VISN 3>VA
New Jersey HCS>Vista

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

The Veterans Health Information System and Technology Architecture (VistA) System is designed to operate as a fully integrated clinical and administrative information source. As such, it processes clinical information, information covered by the Privacy Act & HIPAA (Health Insurance Portability and Accountability Act), PHI/e PHI (*Electronic* and Protected Health Information), financial records, and all other data necessary to run a tertiary medical center. All clinical and most administrative functions within the physical confines of the NJ Data Center utilize the VistA Alpha cluster hosted at the Brooklyn data center to process clinical, financial or

Description of System / Application / Program: administrative data.

VA New Jersey Healthcare
System

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	Privacy Officer:	Helen Hollins	(973) 676-1000 ext 3475
Information Security Officer:	Information Security Officer:	Kathy DeVierno	908 604-5299
Chief Information Officer:	Chief Information Officer:	Scott Soldan	(908) 647-0180 ext. 4615
Person Completing Document:	Person Completing Document:	Kathy DeVierno	908 604-5299
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 08/2008 full PIA and 7/2009 Validation letter
Date Approval To Operate Expires: 08/2008

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301 (a).

What is the expected number of individuals that will have their PII stored in this system: 50,000 to 100,000

Identify what stage the System / Application / Program is at: Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation. 25 years

Is there an authorized change control process
which documents any changes to existing
applications or systems? Yes

If No, please explain:

Has a PIA been completed within the last
three years? Yes

Date of Report (MM/YYYY): 08/2008

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

- | | |
|---|---|
| 1. All System of Record Identifier(s) (number): | 79VA19 |
| 2. Name of the System of Records: | VistA-VA |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://vawww.vhaco.va.gov/privacy/SystemofRecords.htm |

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Healthcare	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Healthcare	Written	Written
Service Information	Paper & Electronic	Benefits	Written	Written
Medical Information	ALL	Healthcare, Research	Written	Written
Criminal Record Information				
Guardian Information	Verbal	Healthcare & healthcare proxy designation	Written	Written
Education Information	Paper & Electronic	Healthcare & employment records	Written	Written
Benefit Information	ALL	Healthcare and benefits	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	Other (Explain)	Voluntary	through Background investigation
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	

Other (Explain)
Other (Explain)
Other (Explain)

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	National VistA Support team	Yes	Dial into the system to resolve issues for a limited amount of time	Both PII & PHI	VA Directive 6500
Other Veteran Organization	VBA	Yes	Compensation & Pension exams	Both PII & PHI	Information is shared through CAPRI and AMIE.
Other Federal Government Agency	DOD	No	Time and leave	PII	DOD – Department of the Army/West Point, NY. Employee information, including names, SS#s, job titles, and number of hours worked. This information is required to complete analysis of employee work hours per pay period. There is a signed DTA to cover the transfer of this information

State Government Agency	State of New Jersey	No	As required by law information is shared with state agencies. A standing order is required to be in place before the information is shared.	Both PII & PHI	Covered by a standing letter with the government agency - †Department of Motor Vehicles (report recurrent periods of loss of consciousness, physical or mental condition that may make a patient an unsafe driver.) Keep unsafe drivers off the roads †Department of Children and Families (report child abuse) We have a responsibility to insure the safety of a child †State Cancer registry (report cancer patients seen at medical center on a monthly basis) The registry tracks Cancer in the state of New Jersey.†Department of Health and Senior Services (report newly diagnosed cases of women with breast cancer) examining relationship of race and risks factors to early age at diagnosis of breast cancer and the aggressiveness of the
Local Government Agency	East Orange/Lyons	No	As required by law information is shared with state agencies. A standing order is required to be in place before the information is shared.	Both PII & PHI	Local legal requirement mandates the release of information and a standing letter would be in effect.
Research Entity	Varies	No	Part of the research protocol	Both PII & PHI	This varies from protocol to protocol. This release would either be consented by the patient or there would be a Data Use Agreement (DUA) in place.

Other Project / System	Social Security Administration	No	release of medical records for processing claims with the Social Security Administration.	Both PHI & Social Security Administration (SSA)	VHA Directive 2010-009, Release of Information to Social Security Administration (SSA)
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?

Yes

Please enter the name of the system: Health Eligibility Center (HEC) and the VHA's Master Patient Index File

Per responses in Tab 4, does the system gather information from an individual?

Yes

If information is gathered from an individual, is the information provided:

Through a Written Request
 Submitted in Person
 Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?

Yes

if yes, please check all that apply:

Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer: The veteran will consent to the use of this data as part of the Research Protocol.

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

Answer:

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

Answer:

VA USE
Department
level the CIO's
Office of
Information
and
Technology
(OI&T) is
responsible for
the
establishment
of directives,
policies, &
procedures
which are
consistent with
the provisions
of Federal
Information
Security
Management
Act (FISMA)
as well as
guidance
issued by the
Office of
Management
& Budget
(OMB), the
National
Institute of
Standards &
Technology
(NIST), &
other
requirements
that VistA-
Legacy is and

Explain what security risks were identified in the security assessment? (Check all that apply)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Computer Misuse |
| <input type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Communications Loss | <input type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Data Destruction | <input type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Theft of Data |
| <input checked="" type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Vandalism/Rioting |
| <input checked="" type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes | <input type="checkbox"/> Burglary/Break In/Robbery |
| <input type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement |
| <input checked="" type="checkbox"/> Flooding/Water Damage | |

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. (Check all that apply)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Risk Management | <input checked="" type="checkbox"/> Audit and Accountability |
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Configuration Management |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Incident Response |
| <input checked="" type="checkbox"/> Physical and Environmental Protection | <input type="checkbox"/> Media Protection |
| <input checked="" type="checkbox"/> Personnel Security | |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: Collection source of data

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?

(Choose One)



The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets



Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?

(Choose One)



The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.



Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?

(Choose One)



The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.



The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	Name	Description	Comments
	<input type="checkbox"/> Is PII collected by this min or application?		
	<input type="checkbox"/> Does this minor application store PII?		
	If yes, where?		
Who has access to this data?			

Minor app #2	Name	Description	Comments
	<input type="checkbox"/> Is PII collected by this min or application?		
	<input type="checkbox"/> Does this minor application store PII?		
	If yes, where?		
Who has access to this data?			

Minor app #3	Name	Description	Comments
	<input type="checkbox"/> Is PII collected by this min or application?		
	<input type="checkbox"/> Does this minor application store PII?		
	If yes, where?		
Who has access to this data?			

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus Mental Health Assistant	BIRLS Centralized Accounts Receivable System (CARS)
Telecare Record Manager	
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill Vocational Rehabilitation & Employment (VR&E) CH 31 Post Vietnam Era educational Program (VEAP) CH 32	INS - BIRLS Mobilization Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS) Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607 Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS Work Study Management System (WSMS)	
Benefits Delivery Network (BDN) Personnel and Accounting Integrated Data and Fee Basis (PAID) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	
SHARE Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

X	ACCOUNTS RECEIVABLE	X	DRUG ACCOUNTABILITY	X	INPATIENT MEDICATIONS	X
	ADP PLANNING (PLANMAN)	X	DSS EXTRACTS		INTAKE/OUTPUT	X
X	ADVERSE REACTION TRACKING		EDUCATION TRACKING	X	INTEGRATED BILLING	
X	ASISTS	X	EEO COMPLAINT TRACKING		INTEGRATED PATIENT FUNDS	X
X	AUTHORIZATION/SUBSCRIPTION	X	ELECTRONIC SIGNATURE	X	INTERIM MANAGEMENT SUPPORT	X
X	AUTO REPLENISHMENT/WARD STOCK	X	ENGINEERING		KERNEL	X
X	AUTOMATED INFO COLLECTION SYS	X	ENROLLMENT APPLICATION SYSTEM		KIDS	X
X	AUTOMATED LAB INSTRUMENTS	X	EQUIPMENT/TURN-IN REQUEST	X	LAB SERVICE	
X	AUTOMATED MED INFO EXCHANGE	X	EVENT CAPTURE		LETTERMAN	X
X	BAR CODE MED ADMIN		EVENT DRIVEN REPORTING	X	LEXICON UTILITY	X
	BED CONTROL		EXTENSIBLE EDITOR	X	LIBRARY	X
X	BENEFICIARY TRAVEL		EXTERNAL PEER REVIEW	X	LIST MANAGER	X
	CAPACITY MANAGEMENT - RUM	X	FEE BASIS		MAILMAN	X
X	CAPRI		FUNCTIONAL INDEPENDENCE	X	MASTER PATIENT INDEX VISTA	X
	CAPACITY MANAGEMENT TOOLS	X	GEN. MED. REC. - GENERATOR	X	MCCR NATIONAL DATABASE	X
X	CARE MANAGEMENT	X	GEN. MED. REC. - I/O	X	MEDICINE	X
X	CLINICAL CASE REGISTRIES	X	GEN. MED. REC. - VITALS	X	MENTAL HEALTH	X
X	CLINICAL INFO RESOURCE NETWORK	X	GENERIC CODE SHEET		MICOM	
X	CLINICAL MONITORING SYSTEM		GRECC	X	MINIMAL PATIENT DATASET	X
X	CLINICAL PROCEDURES		HEALTH DATA & INFORMATICS	X	MYHEALTHEVET	X
X	CLINICAL REMINDERS		HEALTH LEVEL SEVEN	X	Missing Patient Reg (Original) A4EL	X
X	CMOP	X	HEALTH SUMMARY	X	NATIONAL DRUG FILE	X
X	CONSULT/REQUEST TRACKING	X	HINQ	X	NATIONAL LABORATORY TEST	X
X	CONTROLLED SUBSTANCES	X	HOSPITAL BASED HOME CARE	X	NDBI	X
X	CPT/HCPCS CODES	X	ICR - IMMUNOLOGY CASE REGISTRY	X	NETWORK HEALTH EXCHANGE	
X	CREDENTIALS TRACKING	X	IFCAP	X	NOIS	
X	DENTAL	X	IMAGING	X	NURSING SERVICE	
X	DIETETICS	X	INCIDENT REPORTING	X	OCCURRENCE SCREEN	X
X	DISCHARGE SUMMARY	X	INCOME VERIFICATION MATCH	X	ONCOLOGY	
X	DRG GROUPER	X	INCOMPLETE RECORDS TRACKING	X	ORDER ENTRY/RESULTS REPORTING	X

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	Description	Comments
ACCU Care	Patient assessment tool used in <u>Extended Care</u>	
<p><input checked="" type="checkbox"/> YES Is PII collected by this min or application?</p>		
<p><input checked="" type="checkbox"/> YES Does this minor application store PII?</p>		
<p>If yes, where? Server that contained the information is stored in the IT Computer Room.</p>		
<p>Who has access to this data? IT system Administrators and the clinical staff in extended care.</p>		

Minor app #1

Name	Description	Comments
VistA Read Only (Vista RO)	Back-up of VistA information to be used when VistA is down.	
<p><input checked="" type="checkbox"/> YES Is PII collected by this min or application?</p>		
<p>Does this minor application store PII?</p>		
<p><input checked="" type="checkbox"/> YES If yes, where? IT computer room</p>		
<p>Who has access to this data? IT system Administrators and the clinical staff,</p>		

Minor app #2

Name	Description	Comments
Mumps Audio Care	Device that connects to VistA to automatically call veterans to	
<p><input checked="" type="checkbox"/> YES Is PII collected by this min or application?</p>		
<p>Does this minor application store PII?</p>		
<p><input type="checkbox"/> NO If yes, where?</p>		
<p>Who has access to this data? IT s</p>		

Minor app #3

OUTPATIENT PHARMACY	X	SOCIAL WORK
PAID	X	SPINAL CORD DYSFUNCTION
PATCH MODULE	X	SURGERY
PATIENT DATA EXCHANGE	X	SURVEY GENERATOR
PATIENT FEEDBACK	X	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE		TOOLKIT
PCE PATIENT CARE ENCOUNTER		UNWINDER
PCE PATIENT/IHS SUBSET	X	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	X	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	X	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	X	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE		VBECs
POLICE & SECURITY	X	VDEF
PROBLEM LIST	X	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES		VHS&RA ADP TRACKING SYSTEM
PROSTHETICS		VISIT TRACKING
QUALITY ASSURANCE INTEGRATION		VISTALINK
QUALITY IMPROVEMENT CHECKLIST		VISTALINK SECURITY
QUASAR	X	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	X	VOLUNTARY TIMEKEEPING
RECORD TRACKING	X	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	X	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	X	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM RPC BROKER		
RUN TIME LIBRARY SAGG SCHEDULING		
SECURITY SUITE UTILITY PACK		
SHIFT CHANGE HANDOFF TOOL		

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Name	Description	Comments
BCMA Back-up	Contingency PC used when BCMA is not available	
<input checked="" type="checkbox"/>	Is PII collected by this min or application?	
<input checked="" type="checkbox"/>	Does this minor application store PII?	
	If yes, where? Secure PCs on the patient wards.	
	Who has access to this data? IT system administrators and clinical staff who treat the patients.	

Minor app #1

Name	Description	Comments
Health Summary Back-up	Contingency PC that is used when VistA is not available.	
<input checked="" type="checkbox"/>	Is PII collected by this min or application?	
<input checked="" type="checkbox"/>	Does this minor application store PII?	
	If yes, where? Secure PCs on the patient wards.	
	Who has access to this data? IT system administrators and clinical staff who treat the patients.	

Minor app #2

Name	Description	Comments
<input type="checkbox"/>	Is PII collected by this min or application?	
<input type="checkbox"/>	Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Minor app #3

(FY 2010) PIA: Final Signatures

Facility Name: VA New Jersey Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Privacy Officer:	Helen Hollins	(973) 676-1000 ext 3475
Digital Signature Block			
Information Security Officer:	Information Security Officer:	Kathy DeVierno	908 604-5299
Digital Signature Block			
Chief Information Officer:	Chief Information Officer:	Scott Soldan	(908) 647-0180 ext. 4615
Digital Signature Block			
Person Completing Document:	Person Completing Document:	Kathy DeVierno	908 604-5299
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report: 8/1/2008
 OMB Unique Project Identifier 029-00-01-11-01-1180-00
 Region 4>VHA>VISN 3>VA New Jersey HCS>Vista
 Project Name