(FY 2011) PIA: System Identification

Program or System Name:	Region 2 > VHA > VISN 17 > VA Texas Valley Coastal Bend HCS > VistA-VMS
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00
Description of System/ Application/ Program:	Each Veterans Affairs (VA) medical center uses VistA Legacy (formerly DHCP, Decentralized Hospital Computer Program), an integrated hospital information system. DHCP was an M-based internally developed portfolio and VistA Legacy encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms. VistA Legacy is currently running on two core platforms, Microsoft Windows 2000 (W2K)/Cache and Virtual Memory System (VMS)/Cache. This facility operates the following: [ ] InterSystems Cache on Microsoft Windows 2000 [W2K/Cache] [XX] InterSystems Cache on VMS [VMS/Cache]
Facility Name:	VA Texas Valley Coastal Bend Health Care System

Title:	Name:	Phone:	Email:
Privacy Officer:	Donna Gladstone	210-387-0332	donna.gladstone@va.gov
Information Security Officer:	John Reed	210-279-1893	john.reedjr@va.gov
System Owner/ Chief Information Officer:	Ron Cook for BK Hack	817-385-3740	ron.cook1@va.gov
Information Owner:	Jeffery Milligan	956-430-9325	jeffery.milligan@va.gov
Other Titles:	Sara Smith, FCIO	210-831-3982	sara.smith6@va.gov
Person Completing Document:	Donna Gladstone	210--387-0332	donna.gladstone@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			N/A
Date Approval To Operate Expires:			No ATO

What specific legal authorities authorize this program or system:	Title 38 USC, Section 7301 (a)
What is the expected number of individuals that will have their PII stored in this system:	100,000
Identify what stage the System / Application / Program is at:	Implementation
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.	04/2011
Is there an authorized change control process which documents any changes to existing applications or systems?	N/A: First PIA
If No, please explain:	
Has a PIA been completed within the last three years?	N/A: First PIA
Date of Report (MM/YYYY):	03/2011

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 complete TAB 2 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19,
2. Name of the System of Records:	Veterans Health Information Systems and Technology Architecture (VistA) Records-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.rms.oit.va.gov/SOR_Records.asp
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 2011) 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)	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Service Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Medical Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Criminal Record Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Guardian Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Education Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Information will be safe guarded and not given out to anyone.	Verbal & Written	Verbal & Written
Other (Explain)	N/A			

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	Voluntary
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary
Service Information	Yes	Veteran	Voluntary
Medical Information	Yes	Veteran	Voluntary
Criminal Record Information	Yes	Veteran	Voluntary
Guardian Information	Yes	Veteran	Voluntary
Education Information	Yes	Veteran	Voluntary
Benefit Information	Yes	Veteran	Voluntary
Other (Explain)			
Other (Explain)			
Other (Explain)			

4. Notice

(FY 2011) 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	Laredo Vet Center; Corpus Christi Vet Center; McAllen Vet Center	Yes	Medical information to assist with veteran benefit entitlement.	Both PII & PHI	Veteran is required to sign a ROI form.
Other Veteran Organization	N/A				
Other Federal Government Agency	N/A				
State Government Agency	N/A				
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System	N/A				
Other Project / System	N/A				
Other Project / System	N/A				

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
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 2011) 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.	HIV, Research, sickle cell

Answer: An authorization is required from the veteran which states the specific information required.

(FY 2011) 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:

Answer: Data is reviewed by staff

How is data checked for completeness?

Answer: Data is reviewed by staff

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

Answer: When patients come in staff verify patient data

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

Answer: Data is reviewed by staff

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

Answer: N/A

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Patient data is kept indefinitely

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

Answer: health care and benefits

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

Answer: Data is not destroyed

Where are these procedures documented?

Answer: NARA and VHA Handbook 1907.1 and 6300.1 and VA 6500

How are data retention procedures enforced?

Answer: Local policy stating no deletion of Records.

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 2011) 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:

(FY 2011) 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.. No

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? No

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:
Based on VA 6500, testing is completed as required.

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: This facility follows the VA 6500 which requires certification and accreditation documentation including Contingency Plans, Incident Response Plan, Configuration Management Plan, CP testing, Security Configuration Checklists, System Security Plan, Privacy Impact Assessment and applicable Interconnection Security Agreements as necessary.

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

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

☑ Data Destruction

☑ Fraud/Embezzlement

☑ Vandalism/Rioting

Answer: (Other Risks)

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

- ☑ Access Control
- ☑ Audit and Accountability
- ☑ Awareness and Training
- ☑ Certification and Accreditation Security Assessments
- ☑ Configuration Management
- ☑ Contingency Planning
- ☑ Identification and Authentication
- ☑ Incident Response
- ☑ Media Protection
- ☑ Personnel Security
- ☑ Physical and Environmental Protection
- ☑ Risk Management

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: Paper logs have been eliminated as a result of performing the PIA.

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 or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
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 integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of integrity could be expected to have a limited 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 confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of confidentiality could be expected to have a limited 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 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

X Access Manager
Actuarial
X Appraisal System
X ASSISTS
X Awards
Awards
Baker System
X Bbraun (CP Hemo)
BDN Payment History
BIRLS
X C&P Payment System
C&P Training Website
CONDO PUD Builder
Corporate Database
Data Warehouse
EndoSoft
FOCAS
Inforce
INS - BIRLS
X Insurance Online
Insurance Self Service
LGY Home Loans
LGY Processing
Mobilization
Montgomery GI Bill
X MUSE
X Omnicell
X Priv Plus
RAI/MDS
Right Now Web
SAHSHA
X Script Pro
SHARE
SHARE
SHARE
Sidexis
X Synquest
Automated Sales Reporting (ASR)
BCMA Contingency Machines
Benefits Delivery Network (BDN)
X Centralized Property Tracking System
Common Security User Manager (CSUM)
X Compensation and Pension (C&P)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Courseware Delivery System (CDS)
X Dental Records Manager
X Education Training Website
X Electronic Appraisal System
X Electronic Card System (ECS)
X Electronic Payroll Deduction (EPD)
X Eligibility Verification Report (EVR)
Fiduciary Beneficiary System (FBS)
Fiduciary STAR Case Review
X Financial and Accounting System (FAS)
X Insurance Unclaimed Liabilities
X Inventory Management System (IMS)
LGY Centralized Fax System
Loan Service and Claims
Loan Guaranty Training Website
Master Veterans Record (MVR)
Mental Health Asisstant
National Silent Monitoring (NSM)
X Powerscribe Dictation System
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
X Records Locator System
Review of Quality (ROQ)
Search Participant Profile (SPP)
Spinal Bifida Program Ch 18
State Benefits Reference System
State of Case/Supplemental (SOC/SSOC)
Automated Folder Processing System (AFPS)
Automated Medical Information Exchange II (AIME II)
X Automated Medical Information System (AMIS)290
Automated Standardized Performace Elements Nationwide (ASPEN)
Centralized Accounts Receivable System (CARS)
Committee on Waivers and Compromises (COWC)
X Compensation and Pension (C&P) Record Interchange (CAPRI)
Compensation & Pension Training Website
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Distribution of Operational Resources (DOOR)
Educational Assistance for Members of the Selected Reserve Program CH 1606
Electronic Performance Support System (EPSS)
X Enterprise Wireless Messaging System (Blackberry)
X Financial Management Information System (FMI)
Hearing Officer Letters and Reports System (HOLAR)
Inquiry Routing Information System (IRIS)
Modern Awards Process Development (MAP-D)
X Personnel and Accounting Integrated Data and Fee Basis (PAID)
X Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Personnel Information Exchange System (PIES)
Post Vietnam Era educational Program (VEAP) CH 32
Purchase Order Management System (POMS)
Reinstatement Entitelment Program for Survivors (REAPS)
Reserve Educational Assistance Program CH 1607
Service Member Records Tracking System
Survivors and Dependents Education Assistance CH 35
Systematic Technical Accuracy Review (STAR)
Training and Performance Support System (TPSS)
VA Online Certification of Enrollment (VA-ONCE
VA Reserve Educational Assistance Program
Veterans Appeals Control and Locator System (VACOLS)
Veterans Assistance Discharge System (VADS)
Veterans Exam Request Info System (VERIS)
Veterans Service Representative (VSR) Advisor
Vocational Rehabilitation & Employment (VR&E) CH 31
Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

	VBA Data Warehouse	X	Telecare Record Manager		Web Automated Folder Processing System (WAFPS)
	VBA Training Academy		VBA Enterprise Messaging System		Web Automated Reference Material System (WARMS)
	Veterans Canteen Web		Veterans On-Line Applications (VONAPP)		Web Automated Verification of Enrollment
X	VIC		Veterans Service Network (VETSNET)		Web-Enabled Approval Management System (WEAMS)
	VR&E Training Website		Web Electronic Lender Identification		Web Service Medical Records (WebSMR)
	Web LGY				Work Study Management System (WSMS)

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
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

X ASISTS
Bed Control
X CAPRI
X CMOP
X Dental
Dietetics
X Fee Basis
GRECC
X HINQ
X IFCAP
X Imaging
X Kernal
X Kids
X Lab Service
X Letterman
Library
X Mailman
X Medicine
MICOM
NDBI
NOIS
Oncology
X PAID
X Prosthetics
X QUASER
X RPC Broker
SAGG
X Scheduling
X Social Work
X Surgery
X Toolkit
Unwinder
X VA Fileman
VBECS
VDEF
X VistALink

X Beneficiary Travel
X Care Management
X Care Tracker
X Clinical Reminders
X CPT/ HCPCS Codes
X DRG Grouper
X DSS Extracts
Education Tracking
X Engineering
X Event Capture
Extensible Editor
X Health Summary
X Incident Reporting
X Intake/ Output
X Integrated Billing
X Lexicon Utility
X List Manager
X Mental Health
X MyHealthEVet
X National Drug File
X Nursing Service
X Occurrence Screen
X Patch Module
X Patient Feedback
X Police & Security
X Problem List
X Progress Notes
X Record Tracking
X Registration
X Run Time Library
X Survey Generator
X Utilization Review
X Visit Tracking
X VistALink Security
X Women's Health

X Accounts Receivable
X ADP Planning (PlanMan)
X Bad Code Med Admin
X Clinical Case Registries
X Clinical Procedures
X Consult/ Request Tracking
X Controlled Substances
X Credentials Tracking
X Discharge Summary
X Drug Accountability
X EEO Complaint Tracking
X Electronic Signature
X Event Driven Reporting
X External Peer Review
Functional Independence
X Gen. Med. Rec. - I/O
X Gen. Med. Rec. - Vitals
X Generic Code Sheet
X Health Level Seven
X Hospital Based Home Care
Inpatient Medications
Integrated Patient Funds
X MCCR National Database
Minimal Patient Dataset
X National Laboratory Test
X Network Health Exchange
X Outpatient Pharmacy
X Patient Data Exchange
X Patient Representative
X PCE Patient/ HIS Subset
X Security Suite Utility Pack
Shift Change Handoff Tool
Spinal Cord Dysfunction
X Text Integration Utilities
VHS & RA Tracking System
X Voluntary Timekeeping

X Adverse Reaction Tracking
X Authorization/ Subscription
X Auto Replenishment/ Ward Stock
X Automated Info Collection Sys
X Automated Lab Instruments
X Automated Med Info Exchange
Capacity Management - RUM
Capacity Management Tools
Clinical Info Resource Network
Clinical Monitoring System
X Enrollment Application System
X Equipment/ Turn-in Request
X Gen. Med.Rec. - Generator
X Health Data and Informatics
X ICR - Immunology Case Registry
X Income Verification Match
X Incomplete Records Tracking
Interim Mangement Support
X Master Patient Index VistA
X Missing Patient Reg (Original) A4EL
X Order Entry/ Results Reporting
X PCE Patient Care Encounter
X Pharmacy Benefits Mangement
X Pharmacy Data Management
X Pharmacy National Database
X Pharmacy Prescription Practice
X Quality Assurance Integration
X Quality Improvement Checklist
X Radiology/ Nuclear Medicine
X Release of Information - DSSI
X Remote Order/ Entry System
X Utility Management Rollup
CA Vertified Components - DSSI
X Vendor - Document Storage Sys
Visual Impairment Service Team ANRV
X Voluntary Timekeeping National

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 Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?

Name Description Comments Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?

Name Description Comments Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

Facility Name: Region 2 > VHA > VISN 17 > VA Texas Valley Coastal Bend HCS > VistA-VMS

Title:	Name:	Phones:	Email:
Privacy Officer:	Donna Gladstone	210-387-0332	donna.gladstone@va.gov
Information Security Officer:	John Reed	210-279-1893	john.reedjr@va.gov
System Owner/ Chief Information Officer:	Ron Cook for BK Hack	817-385-3740	ron.cook1@va.gov
Information Owner:	Jeffery Milligan	956-430-9325	jeffery.milligan@va.gov
Other Titles:	Sara Smith, FCIO	210-831-3982	sara.smith6@va.gov

Digitally signed by John E Reed Jr
DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=john.reedjr@va.gov, cn=John E Reed Jr
Date: 2011.05.03 12:09:39 -05'00'

Date of Report:	3/1/11
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	Region 2 > VHA > VISN 17 > VA Texas Valley Coastal Bend HCS > VistA-VMS