

Welcome to the PIA for FY 2011!

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.

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/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 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 Directive 6508.
- 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 Directive 6508 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 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 and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect 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

Microsoft Office 2003: 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.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	Development>Enterprise System Manager>Suicide Hotline		
OMB Unique System / Application / Program Identifier	(AKA: UPID #):	None	
Description of System/ Application/ Program:	Provides automated intake processing functionality, record creation, storage, and access for retrieval and further processing. The Suicide Hotline Project is an initiative to collect data from veterans in need and dispatch aid to those veterans that need immediate assistance. Suicide Hotline Project is a suite of applications which facilitate the collection of data from a call center access VISTA data systems and storing the data within a locally hosted database.		
Facility Name:	VA Ann Arbor Healthcare System		
Title:	Name:	Phone:	Email:
Privacy Officer:	Andrea Wilson	321 504-4574	andrea.wilson3@va.gov
Information Security Officer:	Keith Herzberg	321 397-6167	keith.herzberg@va.gov
System Owner/ Chief Information Officer:	Michael Lay		michael.lay@va.gov
Information Owner:	Jan Kemp	585 393-7939	jan.kemp@va.gov
Other Titles:			
Person Completing Document:	Andrea Wilson	321 504-4574	andrea.wilson3@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	No Prior Approved PIA One was done in 2009		
Date Approval To Operate Expires:	No Current ATO		

What specific legal authorities authorize this program or system:	Joshua Omvig Veterans Suicide Prevention Act (HR 5771); VHA Mental Health Strategic Plan. "Suicide Prevention Database-VA" (158VA11)
What is the expected number of individuals that will have their PII stored in this system:	10,000+
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.	2 Years in Operation
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?	No
Date of Report (MM/YYYY):	10/2011

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?
2. Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data? data?

- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data? 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):

158VA11

2. Name of the System of Records:

Suicide Prevention Database VA

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

<http://vaww.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?

No

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?

No

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)	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Service Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Medical Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Criminal Record Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Guardian Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Education Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
Benefit Information	Verbal	Collection is for inclusion in CPRS	Verbally	Verbally
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	VA Files / Databases (Identify file)	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	
Service Information	Yes	Veteran	Voluntary	

Medical Information

It is provided under the disclaimer on the web site, and it is referred to on the Notice of Privacy Practice

Yes	VA Files / Databases (Identify file)	Voluntary
-----	--------------------------------------	-----------

Criminal Record Information	Yes	Veteran	Voluntary
-----------------------------	-----	---------	-----------

Guardian Information	Yes	VA Files / Databases (Identify file)	Voluntary
----------------------	-----	--------------------------------------	-----------

Education Information	Yes	Veteran	Voluntary
-----------------------	-----	---------	-----------

Benefit Information	Yes	Veteran	Voluntary
---------------------	-----	---------	-----------

Other (Explain)

Other (Explain)

Other (Explain)

(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?
Internal Sharing: VA Organization	VHA	Yes	Only information relevant to providing crisis care is obtained	Both PII & PHI
Other Veteran Organization	Various Veteran Service Organizations throughout the Nation	No	Only aggregated data is shared. No personal protected information is shared	N/A
Other Federal Government Agency	Various Federal Agencies to include Department of Defence, U.S. Congress, U.S. Senate	No	Aggregated data is shared. No personal protective information is shared	N/A
State Government Agency	Various State Legislative Offices; States Division of Veterans Affairs	No	Aggregated data is shared. No personal protective information is shared	N/A

Local Government Agency

Various local Legislative
Offices

No

Aggregated data is shared.
No personal protective
information is shared

Research Entity

Other Project / System

Other Project / System

Other Project / System

(FY 2011) PIA: Access to Records

Does the system gather information from another system?

Please enter the name of the system:

VistA

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

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?

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

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: Veteran is referred to their local facility for further treatment

What is the procedure you reference for the release of information?

VHA Handbook 1605.1
Privacy and Release of
Information - Information is
used to provided care

VHA Handbook 1605.1
Privacy and Release of
Information - VHA may use a
limited data set for the
purpose of research, public
health, or health care
operations.

VHA Handbook 1605.1
Privacy and Release of
Information - VHA may use a
limited data set for the
purpose of research, public
health, or health care
operations.

VHA Handbook 1605.1
Privacy and Release of
Information - VHA may use a
limited data set for the
purpose of research, public
health, or health care
operations.

VHA Handbook 1605.1
Privacy and Release of
Information - VHA may use a
limited data set for the
purpose of research, public
health, or health care
operations.

Yes

Yes

Information is provided
verbally

Yes

Yes

Information relating to
purpose of call to suicide
hotline.

(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: Template used to fill out patient information

How is data checked for completeness?

Answer: Intake processing and Suicide Prevention Coordinators at Medical Centers follow up with more specific information as gathered.

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

Answer: Suicide Prevention Coordinators at Medical Centers verify information through VistA and verbally with the Veteran and update VistA as needed

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

Answer: Suicide Prevention Coordinators at Medical Centers verify information through VistA and verbally with the Veteran.

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Per VHA Memorandum 10 -2003-001 and VHA Records Control Schedule (RCS) 10-1, The National Archives and Records Administration (NARA) General Records Schedules (GRSs) - 75 yrs

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

Answer: Meets Federal standards for this type information (VHA Records Control Schedule (RCS) 10-1, The National Archives and Records Administration (NARA) General Records Schedules (GRSs))

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

Answer: Per VHA Records Control Schedule (RCS) 10-1 - Destroy/Delete 75 years after the last episode of patient care.

Where are these procedures documented?

Answer: Department of Veteran Affairs Records Control Schedule 10-1;VHA Memorandum 10 -2003-001, The National Archives and Records Administration (NARA) General Records Schedules (GRSs)

How are data retention procedures enforced?

Answer: through VHA Medical Records Administrators

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.. 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: Security Plan for Ann Arbor and Site Review are included in the C&A package

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

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Blackmail | <input type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Bomb Threats | <input type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Errors (Configuration and Data Entry) | <input type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Communications Loss | <input type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Substance Abuse |
| <input type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Computer Misuse | <input type="checkbox"/> Fraud/Embezzlement | <input type="checkbox"/> Theft of Data |
| <input type="checkbox"/> Data Destruction | | <input checked="" type="checkbox"/> 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: Collection of information considered to be essential to patient health. Controls in place to mitigate misuse of information include controlled access to database, and secure web interface.

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.

adverse effect on operations, assets or individuals.

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

The ultimate objective is to conduct the day-to-day operations of the VA and to accomplish our stated mission with what the Office of Management and Budget (OMB) Circular A-130 defines as adequate security including the magnitude of harm to individuals, the VA, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 low impact defined set of controls.

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 number and your comments.

Tab 3. System of Records: #19 - As of April 14, 2009 a Privacy Notice is being mailed to all veterans enrolled. A privacy notice is not possible at the time personal information is collected because 1) the veteran may not provide personal information and/or 2) The nature of the crisis call may prevent providing a privacy notice.

Tab 5. Data Sharing & Access: #26 - Information is gathered from an individual - submitted in person over the telephone.

Tab 5. Data Sharing & Access: #33 - Will PII be included with any secondary use request - Answer: Yes - Drug/Alcohol Counseling; Mental Health

question you are responding to and then add

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?
--

Access Manager Actuarial Appraisal System ASSISTS Awards Awards Baker System Bbraun (CP Hemo) BDN Payment History BIRLS C&P Payment System C&P Training Website CONDO PUD Builder Corporate Database Data Warehouse EndoSoft FOCAS Inforce INS - BIRLS Insurance Online Insurance Self Service LGY Home Loans LGY Processing Mobilization Montgomery GI Bill MUSE Omnicell Priv Plus RAI/MDS Right Now Web SAHSHA Script Pro SHARE SHARE SHARE Sidexis Synquest	Automated Sales Reporting (ASR) BCMA Contingency Machines Benefits Delivery Network (BDN) Centralized Property Tracking System Common Security User Manager (CSUM) Compensation and Pension (C&P) Control of Veterans Records (COVERS) Control of Veterans Records (COVERS) Control of Veterans Records (COVERS) Courseware Delivery System (CDS) Dental Records Manager Education Training Website Electronic Appraisal System Electronic Card System (ECS) Electronic Payroll Deduction (EPD) Eligibility Verification Report (EVR) Fiduciary Beneficiary System (FBS) Fiduciary STAR Case Review Financial and Accounting System (FAS) Insurance Unclaimed Liabilities 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) Powerscribe Dictation System Rating Board Automation 2000 (RBA2000) Rating Board Automation 2000 (RBA2000) Rating Board Automation 2000 (RBA2000) 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) Automated Medical Information System (AMIS)290 Automated Standardized Performace Elements Nationwide (ASPEN) Centralized Accounts Receivable System (CARS) Committee on Waivers and Compromises (COWC) 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) Enterprise Wireless Messaging System (Blackberry) Financial Management Information System (FMI) Hearing Officer Letters and Reports System (HOLAR) Inquiry Routing Information System (IRIS) Modern Awards Process Development (MAP-D) Personnel and Accounting Integrated Data and Fee Basis (PAID) 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
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
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?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	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

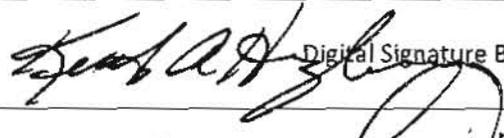
(FY 2011) PIA: Final Signatures

Facility Name: Development>Enterprise System Manager>Suicide Hotline

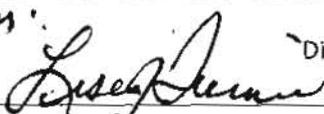
Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:	Andrea Wilson	321 504-4574	andrea.wilson3@va.gov
------------------	---------------	--------------	-----------------------

Information Security Officer:	Keith Herzberg	321 397-6167	keith.herzberg@va.gov
-------------------------------	----------------	--------------	-----------------------


Digital Signature Block 10/19/2011

System Owner/ Chief Information Officer:	Michael Lay	0	michael.lay@va.gov
--	-------------	---	--------------------


Digital Signature Block 10/19/2011

Information Owner:	Jan Kemp	585 393-7939	jan.kemp@va.gov
--------------------	----------	--------------	-----------------

Digital Signature Block

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block

Date of Report: 1/0/00

OMB Unique Project Identifier = '2. System Identification'!D4

Project Name Development>Enterprise System Manager>Suicide Hotline