

| | | |
|--|--|--|
| <u>Welcome to the PIA for FY 2012!</u> | | |
| 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. | | Macros Must Be Enabled To Use Full Functionality For This Form Template! |
| | | 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 <u>Enable Macros at the prompt</u> . Or 1) When file opens click on <u>Enable Macros at the prompt</u> . |
| 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. | | 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 |
| 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. | | <u>Final Signatures</u> |
| | | 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. |
| 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. | | Privacy Impact Assessment Uploaded into SMART All PIA Validation Letters should be mailed to Christina.Pettit@va.gov to receive full credit for submission. |
| <u>INTERNAL WEBSITE</u> : http://vawww.privacy.va.gov/PIA.asp <u>EXTERNAL WEBSITE</u> : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp | | Various Privacy Data Websites: SORNS : http://www.rms.oit.va.gov/SOR_Records.asp Directive Itself (6508): http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=414&FType=2 Schedule FY 2012 : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.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. 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. Chief Information Officer (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) | | |
| Personally Identifiable Information (PII) is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. | | |
| Examples of PII include, but are not limited to: | | |
| • Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number | | |
| • Address information, such as street address or email address | | |
| • Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry) | | |
| • Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information). | | |
| Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. | | |
| A "routine use" is a Privacy Act discretionary authority published in the Federal Register that permits VA to disclose information or records from a Privacy Act-protected record without the patient's prior signed authorization. A "routine use" permits the: | | |
| (1) Release of PHI only when disclosure is also authorized by other applicable legal authorities, including 45 CFR Parts 160 and 164; | | |
| (2) Release of drug or alcohol abuse, HIV, or sickle cell anemia medical information only when the disclosure is also authorized by 38 U.S.C. 7332. | | |

| (FY 2012) PIA: System Information | | *Green Highlight = Must Answer Question | | *Yellow Highlight = Required to Sign PIA | |
|---|--|--|--|--|--|
| Program or System Name (as shown in SMART): | | REGION 3 > VHA > VISN 09 > Memphis VAMC > VistA - VMS | | | |
| OMB Unique System / Application / Program Identifier (AKA: UPID #): | | 029-00-01-11-01-1180-00 | | | |
| Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)" | | <p>VistA is a Major Application as defined by OMB Circular A-130, Appendix III.</p> <p>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.</p> <p>This facility operates the following:</p> <ol style="list-style-type: none"> 1. InterSystems Cache on Microsoft Windows 2000 [W2K/Cache] 2. InterSystems Cache on VMS [VMS/Cache]. <p>VistA Legacy is structured so that it can be customized in certain specialized areas and most local medical centers have taken advantage of this flexibility. Applications within VistA Legacy support a multitude of areas including medical imaging, supply management, decision support, medical research, and education.</p> <p>VHA began deploying DHCP in 1982 with a core set of applications. Today, VistA Legacy is one of the most comprehensive integrated health information systems in the United States. Since episode-of-care workload reporting was an initial motivation for corporate databases, most of VHA's corporate systems collect their information from VistA Legacy. Recent enhancements have clearly shifted the focus from workload to enabling the integration of clinical information from various disciplines, forming the basis for an automated and distributed health information system.</p> | | | |
| Facility or Program Office Name: | | [614] Memphis VA Medical Center | | | |
| Title: | | Name: | | Phone: | |
| Privacy Officer: | | Joseph Boateng, MHIIM, RHIA | | 901-523-8990 x7087 | |
| Information Security Officer: | | Sheila Ervin & McGraff Hurst | | 901-577-7205 901-577-7546 | |
| System Owner/Delegate: | | Jenny Stafford | | 901-523-8990 x5821 | |
| Chief Information Officer: | | Jenny Stafford | | 901-523-8990 x5821 | |
| Information Owner: | | James L. Robinson, III, Psy.D | | 901-523-8990 x 7200 | |
| Other Titles: | | Rodney Schmitz, IT Specialist | | 901-523-8990 x7208 | |
| Person Completing Document: | | Joseph Boateng, MHIIM, RHIA | | 901-523-8990 x7087 | |
| Other Titles: | | | | | |
| Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY) | | | | 11/15/1010 06:24:51 | |
| 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: | | 441630 | | | |
| 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. | | 18 years | | | |
| Is there an authorized change control process which documents any changes to existing applications or systems? | | <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA | | | |
| If No, (Explain on Tab 8) | | | | | |
| Is there a contingency plan in place to process information when the system is down? | | <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA | | | |

| | | | | |
|---|--|--------------------------------------|-------------------------------------|---|
| Has a PIA been completed within the last three years? | | <input checked="" type="radio"/> Yes | <input type="radio"/> No | <input type="radio"/> N/A : First PIA |
| FISMA QUESTIONS | | | | |
| 1. Is this a new system? | | <input type="radio"/> Yes | <input checked="" type="radio"/> No | |
| 2. Does this system contain Federal information in identifiable form? | | <input checked="" type="radio"/> Yes | <input type="radio"/> No | |
| 3. Does the system include information on the public? | | <input checked="" type="radio"/> Yes | <input type="radio"/> No | |
| 4. Is there a Privacy Impact Assessment (PIA) that covers this system? | | <input checked="" type="radio"/> Yes | <input type="radio"/> No | <input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system |
| Identifier? | | <input checked="" type="radio"/> Yes | <input type="radio"/> No | |
| 6. What is the System of Records Notice (SORN) for this system? | | 79VA19 | | |
| 7. Has this SORN been reviewed or updated within the last three years? | | Yes three years ago | | |
| Date of Report (MM/YYYY): | | 30-Oct-09 | | |
| Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions. | | | | |
| If there is no Personally Identifiable Information on your system, please complete TAB 2 & TAB 12. (See Comment for Definition of PII) | | | | |
| <input checked="" type="checkbox"/> Have any changes been made to the system since the last PIA? | | | | |
| <input checked="" type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA? | | | | |
| <input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data? | | | | |
| <input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data? | | | | |
| <input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN? | | | | |
| Directions | | | | |

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

- 1. Is a SORN (System of Records Notice) Required?
- 2. Is there a SORN already in place?

Yes No Not Sure
 Yes No

***If Yes, select all of the appropriate SORN number(s):
***If Not Sure, continue to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

79VA19

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

- 3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

| |
|--|
| <input checked="" type="checkbox"/> Full Name |
| <input checked="" type="checkbox"/> Maiden Name |
| <input checked="" type="checkbox"/> Mother's Maiden Name |
| <input checked="" type="checkbox"/> Alias |
| <input checked="" type="checkbox"/> Social Security Number |
| <input type="checkbox"/> Passport Number |
| <input checked="" type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Taxpayer Identification Number |
| <input checked="" type="checkbox"/> Financial Account Number |
| <input checked="" type="checkbox"/> Credit Card Number |
| <input checked="" type="checkbox"/> Street Address |
| <input checked="" type="checkbox"/> Email Address |
| <input type="checkbox"/> Photographic Image |
| <input type="checkbox"/> Fingerprints |
| <input type="checkbox"/> Handwriting |
| <input type="checkbox"/> Other Biometric Data |
| <input type="checkbox"/> Other (Explain on Tab 8) |

- 4. Based on Question 3, is a SORN required?

Yes No
 Yes No

***If Yes, has the process begun to obtain/acquire a SORN

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

| (FY 2012) PIA: Data Collection And Storage | | *Green Highlight = Must Answer Question | | |
|--|---|--|--|-----------------------------------|
| Please fill in each column for the data types selected. | | | | |
| Data Type | Collection Method | What are the subjects told about the intended use of their information? | 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 | Healthcare | Written | Written |
| Family Relation (spouse, children, parents, grandparents, etc) | Paper & Electronic | Healthcare | Written | Written |
| Service Information | Paper | Healthcare | Written | Written |
| Medical Information | ALL | Healthcare | Written | Written |
| Criminal Record Information | ALL | Healthcare | Written | Written |
| Guardian Information | ALL | Healthcare | Written | Written |
| Education Information | Paper | Healthcare | Written | Written |
| Benefit Information | Paper & Electronic | Eligibility | Written | Written |
| Other (Explain on Tab 8) | | | | |
| Data Type | Storage Method | Source (If requested, identify the specific file, entity and/or name of agency) | Is data collection Mandatory or Voluntary? | |
| Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc) | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Family Relation (spouse, children, parents, grandparents, etc) | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Service Information | <input checked="" type="radio"/> Yes <input type="radio"/> No | Other Federal Agency (Identify) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Medical Information | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Criminal Record Information | <input type="radio"/> Yes <input checked="" type="radio"/> No | | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | |
| Guardian Information | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Education Information | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Benefit Information | <input checked="" type="radio"/> Yes <input type="radio"/> No | VA Files/Databases (Identify File) | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | Automated |
| Other (Explain on Tab 8) | <input type="radio"/> Yes <input checked="" type="radio"/> No | | <input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary | |
| | <i>(Please Select Yes/No)</i> | | | |
| Proximity and Timing: Is the privacy notice provided at the time of data collection? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | |
| Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | |
| Authority: Does the privacy notice specify the effects of providing information on a voluntary basis? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | |
| Disclosures: Does the privacy notice specify routine use(s) that may be made of the information? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | |
| | routine use(s) | | | |

| (FY 2012) PIA: Data Sharing *Green Highlight = Must Answer Question | ** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section. | | | | |
|--|--|---|---|---|---|
| Organization | Name of Agency/Organization | Do they access this system? | Identify the type of Data Sharing | Is PII or PHI Shared? | What is the procedure you reference for the release of information? |
| Internal Sharing: VA Organization | VBA RO; VA RC; | <input checked="" type="radio"/> Yes <input type="radio"/> No | Healthcare | <input checked="" type="radio"/> Yes <input type="radio"/> No | Other (Explain in Tab 8) |
| Other Veteran Organization | Vet Center | <input checked="" type="radio"/> Yes <input type="radio"/> No | Healthcare | <input checked="" type="radio"/> Yes <input type="radio"/> No | Other (Explain in Tab 8) |
| Other Federal Government Agency | | <input checked="" type="radio"/> Yes <input type="radio"/> No | | <input checked="" type="radio"/> Yes <input type="radio"/> No | |
| State Government Agency | State Dept. of Public Health, State Adult & Child Protective Services | <input type="radio"/> Yes <input checked="" type="radio"/> No | Healthcare | <input checked="" type="radio"/> Yes <input type="radio"/> No | Other (Explain in Tab 8) |
| Local Government Agency | State Coroner's Office | <input type="radio"/> Yes <input checked="" type="radio"/> No | Other (Explain in Tab 8) | <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| Research Entity | Pharmaceutical companies. | <input type="radio"/> Yes <input checked="" type="radio"/> No | Other (Explain in Tab 8) | <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| <input checked="" type="checkbox"/> Other Project/ System (Explain on Tab 8) | DoD CDC | No No | BRFSS (Behavior Risk Factor Surveillance System; none | Yes No | VHA handbook 1605.1; Privacy Act SOR Routine Use. |
| (FY 2012) PIA: Access to Records | | | | | |
| Does the system gather information from another system? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | | |
| Please enter the name of the system: | VBA | | | | |
| (FY 2012) PIA: Secondary Use | | | | | |
| Will PII data be included with any secondary use request? | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | | |
| Check all that apply | <input type="checkbox"/> Mental Health | <input type="checkbox"/> HIV | <input type="checkbox"/> Drug/Alcohol Counseling | | |
| | <input type="checkbox"/> Sickle Cell | <input type="checkbox"/> Other (Explain on Tab 8) | <input checked="" type="checkbox"/> Research | | |

| | | | | | |
|---|--|---|--|--|--|
| (FY 2012) PIA: Records Management | | *Green Highlight = Must Answer Question | | | |
| 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? | | | | | |
| <input type="radio"/> Yes (Explain on Tab 8) | | <input checked="" type="radio"/> No | | | |
| Is the data collected to only what is necessary to provide requested service? | | | | | |
| <input checked="" type="radio"/> Yes | | <input type="radio"/> No (Explain on Tab 8) | | | |
| Has the data provided been verified as complete? | | | | | |
| <input checked="" type="checkbox"/> Veteran Verified | | <input type="checkbox"/> Received From Database | <input type="checkbox"/> Verification Unknown | | |
| (FY 2012) PIA: Retention & Disposal | | | | | |
| What is the data retention period? | | RCS 10-1 link for VHA: | www.va.gov/vhapublications/rcs10/rcs10-1.pdf | | |
| 75 years | | RCS VB-1, Part II Revised for VBA: | www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf | | |
| | | National Archives and Records Administration: | www.nara.gov | | |
| Explain why the information is needed for the indicated retention period? | | | | | |
| Answer: mandated by VARCS 10-1 | | | | | |
| What are the procedures for eliminating data at the end of the retention period? | | | | | |
| Deleting records at the end of retention period | | | | | |
| Where are these procedures documented? | | | | | |
| NARA prescribed form: SF-115 | | | | | |
| How are data retention procedures enforced? | | | | | |
| Answer: RCS 10-1 | | | | | |
| Has the retention schedule been approved by the National Archives and Records Administration (NARA)? | | | | | |
| <input checked="" type="radio"/> Yes | | <input type="radio"/> No (Explain on Tab 8) | | | |
| (FY 2012) PIA: Children's Online Privacy Protection Act (COPPA) | | | | | |
| Will information be collected through the internet from children under age 13? | | | | | |
| <input type="radio"/> Yes (Explain on Tab 8) | | <input checked="" type="radio"/> No | | | |

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

| | |
|---|--|
| Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. | <input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8) |
| Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls. | <input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8) |
| Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? | <input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8) |
| Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? | <input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8) |
| Is adequate physical security in place to protect against unauthorized access? | <input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8) |

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

| | | | |
|--|--|---|--|
| <input checked="" type="checkbox"/> Biological Release | <input checked="" type="checkbox"/> Fire | <input checked="" type="checkbox"/> Lightning Strike | <input checked="" type="checkbox"/> Terrorist |
| <input checked="" type="checkbox"/> Blizzard | <input checked="" type="checkbox"/> Flood | <input checked="" type="checkbox"/> Malicious Code | <input checked="" type="checkbox"/> Thunderstorm |
| <input checked="" type="checkbox"/> Burglary/Break In | <input checked="" type="checkbox"/> Hacker / Cracker | <input checked="" type="checkbox"/> Poor/Privacy Negligence | <input checked="" type="checkbox"/> Tornado |
| <input checked="" type="checkbox"/> Civil Unrest | <input checked="" type="checkbox"/> Host | <input checked="" type="checkbox"/> Personnel Unavailable | <input checked="" type="checkbox"/> Tsunami |
| <input checked="" type="checkbox"/> Component Failure | <input checked="" type="checkbox"/> HAZMAT Release/Spill | <input checked="" type="checkbox"/> Power Failure | <input checked="" type="checkbox"/> User Negligence |
| <input type="checkbox"/> Dam Failure | <input checked="" type="checkbox"/> Human Health Emergency | <input checked="" type="checkbox"/> Sabotage | <input checked="" type="checkbox"/> User Sabotage |
| <input checked="" type="checkbox"/> Dust/Debris | <input checked="" type="checkbox"/> Hurricane | <input checked="" type="checkbox"/> System Intrusion, Break-Ins | <input checked="" type="checkbox"/> Vibration |
| <input checked="" type="checkbox"/> Earthquake | <input checked="" type="checkbox"/> HVAC Failure | <input checked="" type="checkbox"/> System Misconfiguration | <input checked="" type="checkbox"/> Volcano |
| <input type="checkbox"/> Extreme Cold | <input checked="" type="checkbox"/> Indoor Humidity | <input checked="" type="checkbox"/> System Penetration | <input checked="" type="checkbox"/> Water Damage |
| <input type="checkbox"/> Extreme Heat | <input type="checkbox"/> Landslide | <input checked="" type="checkbox"/> System Tampering | <input checked="" type="checkbox"/> Winter Weather Hazards |

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. (Check all that apply)

| | | | |
|---|---|---|--|
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> Media Protection | <input checked="" type="checkbox"/> System and Services Acquisition |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security | <input checked="" type="checkbox"/> System and Communication Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection | <input checked="" type="checkbox"/> System and Information Integrity |
| <input checked="" type="checkbox"/> Security Assessment and Authorization | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Assessment | <input checked="" type="checkbox"/> Planning <input checked="" type="checkbox"/> Maintenance |

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the information data types chosen as a basis for your FIPS 199 System Categorization.

Answer: PHI and PII

| | |
|---|---|
| <p>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)</p> | <input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals. |
| <p>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)</p> | <input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals. |
| <p>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)</p> | <input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> 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.

(FY 2012) 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.

Tab 7 (question 12). Security: Explain what security risks were identified in the security assessment? *(Check all that apply)*

Aircraft Crash

Tab 5(4). Reference for information disclosure: VHA Handbook 1605.1

Tab 5 (6). Reference for information disclosure: VHA Handbook 1605.1

Tab 5(10). Reference for information disclosure: VHA handbook 1605.1

Tab 5(12). Reference for information disclosure: VHA handbook

Tab 5(14). Reference for information disclosure: VHA handbook 1605.1; VHA Directive 1200 and VHA handbook 1200.05

(FY 2012) PIA: VBA Minor Applications

| Which of these are sub-components of your system? | | |
|--|--|--|
| Access Manager | Automated Sales Reporting (ASR) | Automated Folder Processing System (AFPS) |
| Actuarial | BCMA Contingency Machines | Automated Medical Information Exchange II (AIME II) |
| Agent Orange | Centralized Property Tracking System | Automated Medical Information System (AMIS)290 |
| Appraisal System | Common Security User Manager (CSUM) | Automated Standardized Performance Elements Nationwide (ASPEN) |
| ASSISTS | Compensation and Pension (C&P) | Broome Closet |
| Awards | Control of Veterans Records (COVERS) | Centralized Accounts Receivable System (CARS) |
| Baker System | Courseware Delivery System (CDS) | Committee on Waivers and Compromises (COWC) |
| Bbraun (CP Hemo) | Dental Records Manager | Compensation and Pension (C&P) Record Interchange (CAPRI) |
| | Education Training Website | |
| | Electronic Appraisal System | Distribution of Operational Resources (DOOR) |
| C&P Payment System | Electronic Card System (ECS) | Educational Assistance for Members of the Selected Reserve Program CH 1606 |
| C&P Training Website | Electronic Payroll Deduction (EPD) | Electronic Performance Support System (EPSS) |
| CONDO PUD Builder | Eligibility Verification Report (EVR) | Enterprise Wireless Messaging System (Blackberry) |
| | Fiduciary Beneficiary System (FBS) | Financial Management Information System (FMI) |
| | Fiduciary STAR Case Review | Hearing Officer Letters and Reports System (HOLAR) |
| EndoSoft | Financial and Accounting System (FAS) | Inquiry Routing Information System (IRIS) |
| FOCAS | Insurance Unclaimed Liabilities | |
| Inforce | Inventory Management System (IMS) | Modern Awards Process Development (MAP-D) |
| INS - BIRLS | Interactive Voce Response (IVR) | Personal Computer Generated Letters (PCGL) |
| Insurance Online | LGY Centralized Fax System | Personnel Information Exchange System (PIES) |
| Insurance Self Service | Loan Service and Claims | Post Vietnam Era educational Program (VEAP) CH 32 |
| LGY Home Loans | Loan Guaranty Training Website | Purchase Order Management System (POMS) |
| LGY Processing | Mental Health Assistant | Reinstatement Entitlement Program for Survivors (REAPS) |
| MES | National Silent Monitoring (NSM) | Reserve Educational Assistance Program CH 1607 |
| Mobilization | Powerscribe Dictation System | RightFax |
| Montgomery GI Bill | Rating Board Automation 2000 (RBA2000) | Service Member Records Tracking System |
| MUSE | Records Locator System | Survivors and Dependents Education Assistance CH 35 |
| Omniceil | Remittance Processing System | Systematic Technical Accuracy Review (STAR) |
| Priv Plus | Review of Quality (ROQ) | Training and Performance Support System (TPSS) |
| RAI/MDS | Search Participant Profile (SPP) | VA Online Certification of Enrollment (VA-ONCE) |
| Right Now Web | Spinal Bifida Program Ch 18 | |
| SAHSHA | State Benefits Reference System | VA Reserve Educational Assistance Program |
| Script Pro | State of Case/Supplemental (SOC/SSOC) | Veterans Assistance Discharge System (VADS) |
| SHARE | Telecare Record Manager | Veterans Exam Request Info System (VERIS) |
| SHARE | | Veterans Insurance Claims Tracking and Response System (VICTARS) |
| Sidexis | | Veterans Service Representative (VSR) Advisor |
| Synquest | VBA Enterprise Messaging System | |
| VBA Training Academy | Web Electronic Lender Identification | Vocational Rehabilitation & Employment (VR&E) CH 31 |
| Veterans Canteen Web | | Web Automated Folder Processing System (WAFPS) |
| VETSNET Housekeeping | | Web Automated Reference Material System (WARMS) |
| VR&E Training Website | | Web Automated Verification of Enrollment |
| Web LGY | | 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 | Not Applicable | |
| Description | | |
| Comments | | |
| Is PII collected by this min or application? | | |
| Does this minor application store PII? | | |
| If yes, where? | Not Applicable | |
| Who has access to this data? | Not Applicable | |
| 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 2012) PIA: Final Signatures | | *Green Highlight = Must Answer Question | |
|---|--|---|-----------------------|
| Facility Name: | [614] Memphis VA Medical Center | | |
| Title: | Name: | Phone: | Email: |
| Privacy Officer: | Joseph Boateng, MHIIM, RHIA | 901-523-8990 x7087 | joseph.boateng@va.gov |
| Digital Signature Block | | | |
| Information Security Officer: | Sheila Ervin | 901-577-7205 | sheila.ervin@va.gov |
| Digital Signature Block | | | |
| System Owner/Delegate: | Jenny Stafford | 901-523-8990 x5821 | jenny.stafford@va.gov |
| Digital Signature Block | | | |
| Chief Information Officer: | Jenny Stafford | 901-523-8990 x5821 | jenny.stafford@va.gov |
| Digital Signature Block | | | |
| Other Titles: | | | |
| Digital Signature Block | | | |
| Date of Report: | 7-May-12 | | |
| OMB Unique Project Identifier | 029-00-01-11-01-1180-00 | | |
| Project Name | FY12-Region3-Memphis VAMC-614-05072012-PIA.xls | | |
| <p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. <ul style="list-style-type: none"> • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmdyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-Region3-Lexington VAMC-596-10302008.xls" • Submit the completed PIA Excel form to SMART Database. • Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmdyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. | | | |