

(FY 2011) PIA: System Identification

Program or System Name: Region 5 > VBA > INS > AITC > General Ledger

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-16-01-1268-00

Description of System/ Application/ Program: General Ledger is a financial recordkeeping and reporting system that records accounting information for all insurance program activities including the disbursements (in the form of debit-credit entities), which have been generated in other insurance subsystems. The data and information that are collected by GL is provided to the Department of Veterans Affairs (VA) Financial Management System (FMS), whereas GL does not make financial disbursements.

General Ledger is supports part of the mission of the Veterans Benefits Administration's (VBA) Insurance program is to provide life insurance benefits to veterans and service members that are not available, under present guidelines, from the commercial insurance industry. Typically, these guidelines prevent and/or limit insurability of the veteran, who is physically or mentally impaired from military service. Benefits and services are typically delivered in an accurate, timely, and courteous manner and at the lowest achievable administrative cost. Insurance coverage is available in reasonable amounts at competitive premium rates. Ultimately, a competitive, secure rate of return wi

Facility Name:	CDCO-AITC, HITC and PITC		
Title:	Name:	Phone:	Email:
Privacy Officer:	Lisa Matuszczak	202-461-9039	Lisa.Matuszczak@va.gov
Information Security Officer:	Connie Hamm	317-916-3408	Connie.Hamm@va.gov
System Owner/ Chief Information Officer:	Kevin C. Causley	202-461-9169	Kevin.Causley@va.gov
Information Owner:	Kevin Causley	202-461-9170	Kevin.Causley@va.gov
Other Titles: C&A Project Officer	Mary D. Barley	202-461-9175	mary.barley@va.gov
Person Completing Document:	Don Burke	512-326-7498	Don.Burke@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			07/2008
Date Approval To Operate Expires:			07/2011
What specific legal authorities authorize this program or system:	USC, section 210(c) and Chapters 11, 13, 15, 31, 34, 35,		
What is the expected number of individuals that will have their PII stored in this system:	10,000,000 - 19,999,999		
Identify what stage the System / Application / Program is at:	Operation/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.	9 Years		

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

If No, please explain:

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

Date of Report (MM/YYYY): 05/2011

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:

36VA00, 36VA29, 46VA00, 53VA00

1. All System of Record Identifier(s) (number):

36VA00: Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA
 36VA29: Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance-VA
 46VA00: Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records-VA
 53VA00: Veterans Mortgage Life Insurance-VA

2. Name of the System of Records:

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?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

No

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Depending on the benefits being requested or provided different personal data will be requested, For example: Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlements and advise about new options. Insured's name, address, bank data (optional), telephone number (optional), insurance file number. This is to contact the veteran policyholder on a scheduled basis in order to pay annual dividends, advise of new or changed benefits, advise of changes to policy status, or request repayment of loan or lien. Name, SSN, Address, Service information, financial information - Determination of entitlement, credit underwriting review, assisting veterans to retain their homes and to perform outreach.

Family Relation (spouse, children, parents, grandparents, etc)

ALL

Loan Guaranty uses personal information to determine if appropriate credit and income standards were used in underwriting the loan. Education-Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement. BIRLS/VADS –

Service Information

Electronic/File Transfer

Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. This information is used to determine eligibility and process entitlement. BIRLS/VADS- uses this information to determine veterans eligibility for VA benefits; uses information such as name, SSN, address, date of birth, service record number, dates of service and any disability ratings.

Medical Information

ALL

Diagnostic codes, percent of disability - Determine eligibility for specially adapted housing, determine appropriate modifications under specially adapted housing program Note: Service connected disability is used to determine if veteran is exempt from funding fees – other than existence of disability determination, no other medical information is used for this purpose.

Criminal Record Information

ALL

Incarceration at a state or local facility, fugitive felon status, investigative reports for some accident. These records are used to suspend benefits during imprisonment at local and Federal facilities.

Guardian Information	ALL	Guardian name, address, telephone number is used to communicate with guardians regarding the veteran or his/her dependent and court proceedings, field examinations, appointments and annual accountings. Guardianship Information may also include court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. It may also include Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status.
Education Information	ALL	Education program approval information on approved courses, effective dates, types of training, facility code, objective code, training type is used during administering education benefits to ensure veterans are in compliance with applicable laws and regulations required to receive benefits.
Benefit Information	ALL	Nothing - Internal systems processing.
Other Rehabilitation	ALL	Diagnostic codes, percent of disability - Determine eligibility for specially adapted housing, determine appropriate modifications under specially adapted housing program.



Data Type	Is Data Type Stored on your system?	Source	(If requested, identify the specific file, entity and/or name of agency)
-----------	-------------------------------------	--------	--

Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran
Service Information	Yes	Veteran
Medical Information	No	
Criminal Record Information	No	
Guardian Information	No	
Education Information	No	
Benefit Information	Yes	Veteran

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

**How is this message
conveyed to them?**

How is a privacy notice provided?

Automated

Automated

Automated

Automated

Automated

Automated

Automated

Automated

All

All

Automated

Automated

Automated

Automated

Automated

Automated



**Is data collection
Mandatory or
Voluntary?**

Additional Comments

The VBA forms include a statement similar to the following: "Important Notice About Information Collection. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you. Personally identifying information you provide will be used only in connection with VA programs and services or for such other purposes as are described at the point of collection." Privacy policy is provided on the website (<http://www.va.gov/privacy/index.htm>). The site specifically states, "You do not have to give us personal information to visit our site. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you."

Voluntary

Voluntary

Mandatory

Voluntary



(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	1. VA Regional Office and Insurance Center (VAROIC) Operations Division 2. Veterans Affairs Central Office (VACO)	Yes	1. Accounting information is transferred from PITC to the AITC Mainframe system. 2. End-of-Month processing entries.	PII	All information is held internally to the system.
Other Veteran Organization	No				
Other Federal Government Agency	No				
State Government Agency	No				
Local Government Agency	No				
Research Entity	No				
Other Project / System	No				
Other Project / System	No				
Other Project / System	No				

(FY 2011) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	REGION5> VBA> C&P> AITC> BIRLS/VADS	
Per responses in Tab 4, does the system gather information from an individual?		No
If information is gathered from an individual, is the information provided:	<input type="checkbox"/> Through a Written Request <input type="checkbox"/> Submitted in Person <input type="checkbox"/> 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?	No
---	----

Drug/Alcohol Counseling Mental Health HIV

if yes, please check all that apply:

Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(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: The General Ledger application is under configuration control and only approved processing requirements, to include data collection, are analyzed and approved. DVA requires minimal identifying information for BIRLS records. In accordance with GPRA of 1993. DVA reviews forms at regular intervals and removes any request for data elements no longer needed. Electronic data transfers are subject to design criteria, industry format standards and automated checks to ensure that only appropriate data is contained in the transfer.

How is data checked for completeness?

Answer: Data received via via Electronic Transfer by General Ledger is treated as complete and vetted. On Line Transaction Processing (OLTP) entries are parsed, programmatically, to ensure completeness and correctness.

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

Answer: Data collected and stored by General Ledger relies on the policies, procedures and processing of external entities to data correctness.

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

Answer: Data collected and stored by General Ledger relies on the policies, procedures and processing of external entities to data correctness.

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: VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures. General Ledger records are retained indefinitely.

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

Answer: Although there are other data storage mechanisms throughout the US government IT infrastructure for preserving veterans information, General Ledger maintains a virtual accounting of Veteran's Insurance information.

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

Answer: The data retention period for BIRLS data is contained in RCS VBA-1, Part I, Item Number 08-065.000

Where are these procedures documented?

Answer: For insurance records: Philadelphia ITC Operating Memorandum 284-07-00, Subj: Protection of VA Indispensable Records and Philadelphia ITC Operating Memorandum 284-16-05, SUBJ: Direct Access Storage Device (DASD) Management.

How are data retention procedures enforced?

Answer: Active insurance records are retained. Data on active records is changeable. Prior copies of active records and their changing values are not retained. Inactive records are purged from some applications, but the record as it appeared at its final active day is retained. A list of transactions affecting the system has been maintained since 1995 and there are no plans to remove records. The records retention program requires storage of inactive records at a servicing Federal Archives and Records Center for 50 years. Life insurance programs for veterans have been in force since 1919. It is not uncommon for VA to receive inquiries about old insurance policies. For instance, we receive frequent inquiries about military and VA insurance paperwork found in the effects of deceased veterans. Occasionally, these date back several years, and in a few well-publicized cases to deaths that occurred in WW II. To the extent these records can be retrieved and/or reconstructed, we can discharge our duty to those veterans and their families.

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? No

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

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

Answer: On an annual basis, the VA Chief Information Officer (CIO), in conjunction with system owners and information owners, and with advice from the VA Office of Inspector General (OIG), evaluate the Department's overall IT security posture. This evaluation includes identification of significant security performance gaps, the prioritization of key POA&M weakness areas for immediate remediation action, as well as the designation of certain security areas that would benefit from enterprise-wide management of a single security solution, thereby effectively targeting those areas for action that would most improve the Department's security posture in the nearterm.

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: A standardized Department methodology based on the direction in National Institute of Standards and Technology (NIST) guidance is used to continuously monitor, test and evaluate security for this major application. The approximately 60 common security controls provided by the Office of Information and Technology (OIT), or other respective VA Program Office, are tested every year. Application-specific security testing evaluates approximately one-third of the remaining 90 controls on an annual basis, with the entire respective application NIST Special Publication (SP) 800-53 security control baseline—at the Federal Information Processing Standard (FIPS) 199 level of moderate--being tested over each three-year period. The testing supports certification and re-accreditation requirements, as well as Federal Information Security Management Act (FISMA) requirements to annually test the operational, management, and technical controls of each Department system. The specific controls identified for testing are selected by OIT Operations, with advice from the VA Office of Cyber Security (OCS).

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

7. Security

- 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

Answer: (Other Risks)

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

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: No changes to the application or the method of collection of information will be made as a result of performing this 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)

- | | |
|-------------------------------------|---|
| <input 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 checked="" 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. |

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)

- | | |
|-------------------------------------|--|
| <input 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 checked="" 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. |

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)

- | | |
|-------------------------------------|--|
| <input 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 checked="" 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 VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. 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 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

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?
--

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 Assistant 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	Agent Cashier	Administrative Data Repository (ADR)
A4P	Air Fortress	Automated Access Request
ADT	Auto Instrument	Bed Board Management System
BDN 301	Cardiff Teleform	Cardiology Systems (stand alone servers from the network)
CP&E	CHECKPOINT	Clinical Data Repository/Health Data Repository
DRM Plus	Data Innovations	Combat Veteran Outreach
DSIT	DELIVEREX	Committee on Waiver and Compromises
ENDSOFT	DSS Quadramed	Crystal Reports Enterprise
EYECAP	EKG System	DICTATION-Power Scribe
Genesys	ePROMISE	EDS Whiteboard (AVJED)
ICB	Lynx Duress Alarm	Embedded Fragment Registry
KOWA	Mumps AudioFAX	Enterprise Terminology Server & VHA Enterprise Terminology Services
MHTP	Onvicord (VLOG)	Financial and Accounting System (FAS)
NOAHLINK	P2000 ROBOT	Financial Management System (FMS)
Omnicell	PACS database	Health Summary Contingency
Optifill	PIV Systems	Microsoft Active Directory
PICIS OR	Remedy Application	Microsoft Exchange E-mail System
Q-Matic	Traumatic Brain Injury	Military/Vet Eye Injury Registry
RAFT	VAMedSafe	Personal Computer Generated Letters
RALS	VBA Data Warehouse	QMSI Prescription Processing
SAN	VHAHUNAPP1	Scanning Exam and Evaluation System
Sentillion	VHAHUNFPC1	Tracking Continuing Education
Stellant	VISTA RAD	VA Conference Room Registration
Stentor	Whiteboard	

Explain any minor application that are associated with your installation that does not appear in the list above. Please

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: Final Signatures

Facility Name: Region 5 > VBA > INS > AITC > General Ledger

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

Privacy Officer:	Lisa Matuszczak	202-461-9039	Lisa.Matuszczak@va.gov
------------------	-----------------	--------------	------------------------

Signature not verified!	Lisa M. Matuszczak	Digitally signed by: Lisa M. Matuszczak DN: CN = Lisa M. Matuszczak C = US O = U.S. Government OU = Department of Veterans Affairs Date: 2011.05.31 08:37:23 -05'00' Reason: I am approving this document
-------------------------	--------------------	---

Information Security Officer:	Connie Hamm	317-916-3408	Connie.Hamm@va.gov
-------------------------------	-------------	--------------	--------------------

	Digital Signature Block	5-31-11
---	-------------------------	---------

System Owner/ Chief Information Officer:	Kevin C. Causley	202-461-9169	Kevin.Causley@va.gov
--	------------------	--------------	----------------------

Digital Signature Block

Other Titles: C&A Project Officer	Mary D. Barley	202-461-9175	mary.barley@va.gov
-----------------------------------	----------------	--------------	--------------------

Digital Signature Block

Date of Report: 05/2011
OMB Unique Project Identifier: 029-00-01-16-01-1268-00
Region 5 > VBA > INS > AITC >
Project Name: General Ledger