

## **Welcome to the PIA for FY 2010!**

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

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

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

### **Directions:**

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

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

PIA Website: [http://vaww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vaww.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 Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

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

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

## (FY 2010) PIA: System Identification

Program or System Name: First Party Lockbox Payments (LBX)

OMB Unique System / Application / Program Identifier (AKA: UPID #): not available yet

Description of System/ Application/ Program: The LBX system resides on the Enterprise Server at the AITC. LBX receives first party medical payment transactions from Bank of America and transmits these payments to corresponding VA Medical Center (VAMC's). Exception items (payments received without a coupon or account number) are placed on the Lockbox workload menu for the exception team to research and find the correct account number. LBX interfaces and provides data to other applications

Facility Name:	CDCO Austin		
<b>Title:</b>	<b>Name:</b>	<b>Phone:</b>	<b>Email:</b>
Privacy Officer:	Amy Howe	512-326-6217	<a href="mailto:amy.howe1@va.gov">amy.howe1@va.gov</a>
Information Security Officer:	Jarrold Tillman	202-461-6381	<a href="mailto:Jarrod.Tillman@va.gov">Jarrod.Tillman@va.gov</a>
Chief Information Officer:	Judy Downing	512-326-6000	<a href="mailto:judy.downing@va.gov">judy.downing@va.gov</a>
Person Completing Document:	Greg Watson	512-326-6889	<a href="mailto:Gregory.Watson@va.gov">Gregory.Watson@va.gov</a>
Other Titles:	Ernest Washington	(202) 461-1625	<a href="mailto:ernest.washington@va.gov">ernest.washington@va.gov</a>
Other Titles:	Sergio Falcon	512/326-6628	<a href="mailto:sergio.falcon@va.gov">sergio.falcon@va.gov</a>
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	n/a		
Date Approval To Operate Expires:	n/a		

What specific legal authorities authorize this program or system:

Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, April 7, 1986, allowed VA to bill health insurance companies for all nonservice-connected (NSC) veterans. The law also established the Means Test Program. Means testing enables the VA to categorize veterans, according to income, and to collect appropriate copayments for outpatient and inpatient healthcare services.

What is the expected number of individuals that will have their PII stored in this system:

Approximately 2 to 3 million.

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

Implementation

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

10 years

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

N/A: First PIA

If No, please explain:

Has a PIA been completed within the last three years?

No

Date of Report (MM/YYYY):

03/2010

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

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

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

## (FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? 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): 114VA16, 114VA17, 79VA19, 88VA20A6, 88VA244
2. Name of the System of Records: Accounts Receivable Records-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL): <http://federalregister.gov/Privacy/va.aspx>

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?

No

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

No

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?

No

## (FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	used for payment research purposes	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information	VA File Database	used for payment research purposes	Written	Written
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
Other (Explain)	Electronic/File Transfer	Yes - by Bank of America (collector of information)	Automated	Written

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)	Mandatory	info comes from CCPC
Family Relation (spouse, children, parents, grandparents, etc)				

Service Information

---

Medical Information

Yes

VA Files / Databases (Identify file)

Mandatory

info comes from  
CCPC

---

Criminal Record Information

---

Guardian Information

---

Education Information

---

Benefit Information

---

Other (Explain)

Yes

Other (Explain)

Mandatory

info comes from  
Bank of America

---

Other (Explain)

Other (Explain)

---

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Medical Centers	No	Payment information is transmitted for posting to corresponding Veteran accounts at each VA Medical Center.	Both PII & PHI	n/a
Other Veteran Organization	FSC	Yes	Staff has access to payment and Veteran data. They used this info to resolve unidentified payment items.	Both PII & PHI	n/a
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	Consolidated Co-Payment Processing Center (CCPC)	
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 2010) 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 2010) PIA: Program Level Questions

---

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

No

If Yes, Please Specify:

---

Explain how collected data are limited to required elements:

Answer: Data elements are limited to data obtained through file transfer from Bank of America and CCPC. Subroutines were developed to provide only the data necessary for accountability and payment processing.

---

How is data checked for completeness?

Answer: Data received from Bank of America (BOA) is verified prior to importing data into the LBX system. Validity checks are used along with header records providing expected payment amounts data validation and edits are also performed to validate integrity of the data received.

---

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

Answer: Job scripts have been developed to archive data after 15 months. Data is then held in archive for a period of seven years and purged/sanitized according to VA Handbook and Directive 6500 based on policy controls for retention of backup media for the system.

---

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

Answer: System subroutines perform data validation checks and cross reference to existing data to ensure relevancy as well as file transfer protocol checksum validation utilities are utilized to ensure data transmission is free of errors and anomalies.

---

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

Answer:

---

## (FY 2010) PIA: Retention & Disposal

---

What is the data retention period?

Answer: Seven (7) years

---

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

Answer: Financial accountability

---

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

Answer: IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not accessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

---

Where are these procedures documented?

Answer: VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

---

How are data retention procedures enforced?

Answer: No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

---

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

---

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

Answer:

---

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

---

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

No

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

Answer:

---

## (FY 2010) PIA: Security

---

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

Yes

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

No

---

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

Yes

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

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: Prior to production, a Certification and Accreditation with the Authority to Operate will be complete. Prior to receiving access, the user must complete and sign User Access Request Form. The user acknowledges and signs he/she will abide by the Rules of Behavior. The user also must complete mandatory security and privacy awareness training. Separate Rules of Behavior will be established for the application/system administrators with privileged accounts, including application, database, and alternate system administrators.

---

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

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

Answer: (Other Risks)

---

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

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

Answer: (Other Controls)

---

## PIA: PIA Assessment

---

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

Answer: None

---

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 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.

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

**(Choose One)**

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

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

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

*Please add additional controls:*

**(FY 2010) PIA: Additional Comments**

---

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

---

(FY 2010) PIA: VBA Minor Applications

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

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

---

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

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

Minor app #1	Name		Description	Comments
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	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?		

Minor app #3	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 2010) PIA: VISTA Minor Applications

---

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

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

---

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

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

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

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

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

(FY 2010) PIA: Minor Applications

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

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

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

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

## (FY 2010) PIA: Final Signatures

Facility Name: CDCO Austin

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Digital Signature Block			
Information Security Officer:	Jarrod Tillman	202-461-6381	Jarrod.Tillman@va.gov
Digital Signature Block			
Chief Information Officer:	Judy Downing	512-326-6000	judy.downing@va.gov
Digital Signature Block			
Person Completing Document:	Greg Watson	512-326-6889	Gregory.Watson@va.gov
Digital Signature Block			
System / Application / Program Manager:	Ernest Washington	(202) 461-1625	ernest.washington@va.gov
Digital Signature Block			

Date of Report: 3/1/2010  
 OMB Unique Project Identifier: not available yet

Project Name: First Party Lockbox Payments (LBX)

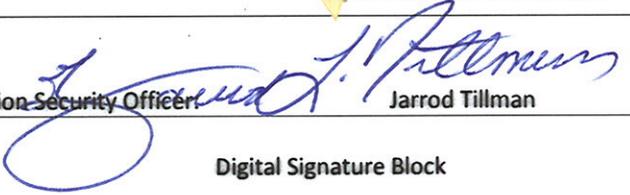
### (FY 2010) PIA: Final Signatures

Facility Name: CDCO Austin

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

Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
------------------	----------	--------------	------------------

<b>AMY HOWE</b>	Digital Signature Block Digitally signed by: AMY HOWE DN: CN = AMY HOWE O = Department of Veterans Affairs, Internal Staff Date: 2010.03.25 10:17:59 -06'00'
-----------------	---

Information Security Officer:	 Jarrod Tillman	202-461-6381	Jarrod.Tillman@va.gov
-------------------------------	--	--------------	-----------------------

Digital Signature Block
-------------------------

Chief Information Officer:	Judy Downing	512-326-6000	judy.downing@va.gov
----------------------------	--------------	--------------	---------------------

Digital Signature Block
-------------------------

Person Completing Document:	Greg Watson	512-326-6889	Gregory.Watson@va.gov
-----------------------------	-------------	--------------	-----------------------

Digital Signature Block
-------------------------

System / Application / Program Manager:	Ernest Washington	(202) 461-1625	ernest.washington@va.gov
---	-------------------	----------------	--------------------------

Digital Signature Block
-------------------------

Date of Report: 3/1/2010  
OMB Unique Project Identifier: not available yet

Project Name: First Party Lockbox Payments (LBX)