Privacy Impact Assessment for the VA IT System called:

Veterans Health Administration

Laboratory System Reengineering Project (LSRP)

Date PIA submitted for review:

02/24/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Diana Bowen	Diana.Bowen@va.gov	304-429-6741 X3609
Information System Security Officer (ISSO)	Craig Heitz	craig.heitz@va.gov	612-725-2132
Information System Owner	Christopher Brown	christopher.brown@va.gov	716-782-3294
Person Completing the Document	James McIntyre	James.Mcintyre2@va.gov	913-300-2055

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The purpose of this project is to replace the legacy Laboratory Information Management System (LSRP) with a Commercial Off-The-Shelf (COTS) LSRP. The selected COTS product and managed service, Cerner Millennium PathNet Remote Hosting Option (RHO) that resides at the Cerner Technology Centers in Kansas City, will allow the VA to meet future requirements of Electronic Medical Record, HealtheVet and interoperability between the Department of Defense (DoD) and Public Health Services (PHS) as per public law 107-287.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*

- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*
- *The VHA Laboratory Service is a critical part of offering high quality clinical care to veterans. Almost 80% of clinical decisions are based on the patient's laboratory test results which have increased an average of 5% annually and approximately 30% since 2001. The selected COTS replacement and managed service exceeds the functional requirements of the VA Laboratory community, supports the reengineered business processes, requires no software code modifications to the COTS LSRP and will move laboratory information from locally maintained records to "patient focused" (portability of information to another facility). The project supports the VA strategic goal of providing high-quality, reliable, accessible, timely, and efficient health care that maximizes the health and functional status of enrolled veterans.*

The **Laboratory System Reengineering Project (LSRP)** is intended to replace the existing Laboratory Information Management System (LSRP) with a Commercial Off-The-Shelf (COTS) LSRP. The selected system consists of the COTS software solution, Cerner Millennium PathNet, as well as the Cerner Remote Hosting Option (RHO) managed service. The RHO option includes the hosting and management of the LSRP system from the Cerner Technology Centers in Kansas City, Missouri. The VA retains all ownership over the data processed by the LSRP.

The LSRP automates laboratory workflows by interfacing with other VA Health Information System clinical and revenue-cycle workflows to process lab test orders, manage specimens, support laboratory quality checks, and support the delivery of test results to the appropriate clinical systems and providers to enable effective and efficient care delivery. The LSRP also supports laboratory test order processing workflows for 3rd party laboratory testing services. The COTS LSRP and RHO manages service enables the VA to meet future requirements of Electronic Medical Record, HealtheVet and interoperability between the Department of Defense (DoD) and Public Health Services (PHS) as per public law 107-287. The system is expected to hold the laboratory data of approximately 40,000 Veterans.

The LSRP system processes the PII and PHI of all VA patients who receive laboratory services from the VA. The data processed by the LSRP includes: VA Veteran or primary subject's personal contact information (name, address, telephone, etc.); personal identifiers (Social Security Number (SSN), financial account number); family relation; service information; medical record information. Records can be retrieved using full name, SSN, and financial account number. Records can also be retrieved via searches on Medical Record Number, birth date, gender, and unique identifiers assigned by the LSRP (accession numbers)

Given the potential quantity and the sensitivity of the data, the potential impact of unauthorized access or disclosures of the data processed by the LSRP is significant for the VA, the managed service provider, and the patients.

All of the PII and PHI processed by the LSRP is received from VistA as well as Quest Diagnostics and LabCorp Reference Lab systems via HL7 interfaces.

The legal authority to operate the system falls under Title 38, United States Code, Section 501.

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Other Unique Identifying Number (list below)

- Family Relation (spouse, children, parents, grandparents)
- Service Information
- Medical Information
- Laboratory test orders and results

PII Mapping of Components

LSRP consists of 1 key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **LSRP** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Millennium	Yes	Yes	Referenced above	Perform laboratory test for the purpose of medical diagnosis and treatment	800-53 rev 4 High Baseline, HIPAA security and privacy rules

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All of the PII processed by the LSRP is received from VistA as well as Quest Diagnostics and LabCorp Reference Lab systems via HL7 interfaces. The LSRP does not collect data directly from a patient.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All of the PII and PHI processed by the LSRP is received from VistA as well as Quest Diagnostics and LabCorp Reference Lab systems via HL7 interfaces.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

The selected COTS replacement and managed service exceeds the functional requirements of the VA Laboratory community, supports the reengineered business processes, requires no software code modifications to the COTS LSRP and will move laboratory information from locally maintained records to "patient focused" (portability of information to another facility). The project supports the VA strategic goal of providing high-quality, reliable, accessible, timely, and efficient health care that maximizes the health and functional status of enrolled veterans.

1.5 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The LSRP provides the capability to support workflows that include manual order review and quality checks. The LSRP relies on the underlying integrity and accuracy of the data provided by source systems.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

On behalf of Huntington VAMC, Cerner is authorized to collect the information described in question 1.1 under the Veterans Benefits Act, Chapter 73: Veterans Health Administration – Organization and Functions, Title 38, U.S.C. § 7301;
SORN 24VA19 and Executive Order 9397 authorize the collection and use of SSNs. There is a fully executed ISA/MOU in place between LSRP and the VA.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk:

Both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI) is collected. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation:
A variety of security measures designed to ensure that the information is not inappropriately disclosed or released is employed. These measures 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 National Institute of Standards and Technology (NIST) Special Publication 800-37.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

The information collected will be used to provide high quality laboratory services in support of the VA's mission of utilizing high quality, effective, and efficient Information Technology services to provide benefits and services to the Veterans of the United States.
Name – Used to identify the patient during appointments and in other communication.
Social Security Number – Used as a patient identifier.
Date of Birth – Used to identify age and confirm patient identity
Mailing Address – Used as a patient identifier
Phone Number – Used as a patient identifier
Health Insurance – Used to link records between LSRP and VISTA systems.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring,

reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Results from laboratory services are appended to the patient's current record in VistA.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

LSRP provides the capability to limit access to patient information to authorized users of the LSRP through role-based access control. The LSRP provides security and user event logging including the actions taken by users on the data.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Veteran or primary subject's personal contact information (name, address, telephone, etc.); family relation; service information; medical information. Records can be retrieved using full name, SSN, and financial account number. Records can also be retrieved via searches on accession number, Medical Record Number, birth date, and gender.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1. Retention period for the PHI is 75 years after date of last episode of patient care.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

Yes, VA Records Control Schedule 6000.2(b) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf)

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

Prior to termination or completion of this contract, Cerner LSRP and their affiliated business partners must receive written approval from the VHA before any VA/VHA provided information is destroyed. Any data destruction done on behalf of the VA/VHA must be done in accordance with National Archives and Records Administration (NARA) approved records schedules found in VHA RCS 10-1.
Destroyed in accordance with records control schedule making the data unidentifiable. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008),
http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.
Huntington VAMC additionally follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for MediaSanitization Program,
https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/IS%20Reference%20Guide%20%20Doc%20Library/SOPs%20-%20FSS/FSS%20SOP%20MP-6%20Electronic%20Media%20Sanitization%20v3.6.pdf as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research:

Veterans may obtain medical records with a written request or on VA Form 10-5345a. Veterans may also view their medical records on My HealtheVet, after signing up. The facility that the veteran receives his/her care provides a First-party right of access to records contained in the Privacy Act SOR. Police Reports (UORs) are requested via Freedom of Information Act (FOIA); however, other records are requested in writing through the Privacy Officer. Access to any non-medical record will

be directed to the Privacy Officer. Requests to review medical records in their original form will be processed by the Privacy Officer. The facility where the veteran receives their care has a Release of Information department processes medical records requests for veterans, third and first parties. The VA Form 10-5345 is used for the Veteran to authorize disclosure to third parties. The Privacy Officer conducts monitors of the Release of Information, which is reported to VHA Privacy Compliance Assurance team quarterly.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk:
The risk associated with storing this data increases the longer the data is stored.

Mitigation:
To mitigate the risk posed by information retention, Cerner LSRP adheres to the VA RCS schedules for each category or data it maintains. When the retention date is reached for a record, the medical center and Cerner LSRP will carefully dispose of the data by the determined method as described in RCS 10-1

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VistA	Laboratory services	PHI/PII	HL7

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

Commercial testing laboratories have PHI and PII data exposure risk when handling VA patient information.

Mitigation:

Commercial testing laboratories follow Health and Human Services (HHS) Health Insurance Portability and Accountability Act (HIPAA) guidelines and practices in the handling and management of patient data https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: This question is #7 in the Privacy Threshold Analysis.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Quest Diagnostics	Lab orders may be transmitted to and results received from Quest if facility is used	PHI (MRN only)	SORN 24VA19	HL7
LabCorp Reference Lab	Lab orders may be transmitted to and results received from LabCorp if facility is used	PHI (MRN only)	SORN 24VA19	HL7
Cerner (LSRP)	To automate laboratory workflows by interfacing with other VA Health Information System clinical and revenue-cycle workflows.	PII/PHI	ISA/MOU in place between VA and Cerner LSRP	HL7

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

NIST standard 800-53 rev 4 high baselines implemented for the system as well as going through the authorization process.
The following measures are currently being taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16:
• Secure complex passwords are required, authentication codes are required, and authorized access with PIV badge or VA-approved 2FA are the only access methods in order to protect Veterans personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
• The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

• The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
• The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
• Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk:
Commercial testing laboratories have PHI and PII data exposure risk when handling VA patient information.

Mitigation:
Commercial testing laboratories follow Health and Human Services (HHS) Health Insurance Portability and Accountability Act (HIPAA) guidelines and practices in the handling and management of patient data. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Notice:
The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf
2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

LSRP does not collect information directly from the patient.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

LSRP does not collect information directly from the patient.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk:

There is a risk that veterans and other members of the public will not know that the Cerner LSRP exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation:

Cerner LSRP mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the System of Record Notice

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf
2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this

section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals must follow established procedures to gain access to their information under the guidelines of the Privacy Act, Freedom of Information Act (FOIA), and Health Insurance Portability and Accountability Act (HIPAA).
When requesting access to one's own records, patients are asked to complete VA Form I 0-5345a: Individuals ' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vafonns/medical/pdf/vha-10-5345a-fill.pdf.
Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealtheVet program, VA's online personal health record. More information about MyHealtheVet is available at https://www.myhealth.va.gov/index.html.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

When a Veteran has concerns that something written in his/her medical records is inaccurate, incomplete or needs to be removed entirely, they have the right to request an amendment of the record. The Veteran must submit their request in writing, specify the information that they want corrected, and provide a reason to support the request for amendment. All amendment requests must be submitted to the facility Privacy Officer.
The Privacy Officer refers the request and related record to the health care provider who authored the information in order for the provider to determine if the record needs to be amended as requested. If the author is not available, the documentation is referred to that provider's supervisor.
If the amendment is granted, the facility Privacy Officer will work with the responsible record custodian to amend their records. If the amendment is not granted, the Privacy Officer will notify the Veteran of the decision and include appeal rights.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The facility staff and providers are educated to refer the Veteran to the Privacy Officer for requests to correct their records. At the time of the request the individual is sent an acknowledgement letter and they are sent a letter at the completion of processing regarding the outcome of the requested correction.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Redress is provided through the Privacy Act for the individual to view and request correction to the inaccurate or erroneous information. If the request is denied, the individual may appeal the decision by writing to the Office of General Counsel (024); Department of Veterans Affairs; 810 Vermont Avenue, N.W.; Washington, D.C. 20420.
The Privacy Act and HIPAA permit the individual to also complete a Statement of Disagreement to the information that was denied correction. The facility would be able to include a rebuttal to the Statement of Disagreement. The Statement of Disagreement, rebuttal, and denial letter would be attached to the information that was requested to be corrected and would be released with the information at any time the information was authorized for release.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk:
If a system does not allow individual access, the risk of inaccurate information may occur. Additionally, patients should have access to the information so they can keep abreast of labs which are outside of normal and plan their healthcare accordingly. If a healthcare provider depends on inaccurate information, the patient could be given the wrong treatment.

Mitigation:
The Privacy Risk is low-moderate, as the information is processed through the Privacy Act, HIPAA, and FOIA. FOIA protects specific records with exemptions. When information is processed under FOIA, the exemptions and an explanation of the exemption are included in the response to the request. The individual has a right to access their individual information under the Privacy Act, when that information is part of a Privacy Act System of Records. An individual's identity is confirmed in requesting access, redress, and correction of information through legal authority (POA, Guardian, Next of Kin), photo identification and/or wet signature, which protect the information from being used without the individual's knowledge. Appeal rights are given to an individual upon denial of a correction.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Types of accounts are defined as being "named accounts" and "support accounts". "Named accounts" have rights and privileges based on a pre-determined profile for an individual's role. "Support accounts" are temporary and provide short-term access for troubleshooting or project-oriented work on a client's processing environment. These accounts, generated by Cerner Technology Services (CTS) Enterprise Security Identity Access Management, grant limited access appropriate to the type of troubleshooting and/or project work required as outlined in the Performance Work Statement.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Only VA-approved Cerner contractor personnel will be able to access the data. Approved personnel will go through the VA onboarding process, receive a clearance, and complete required training before access is granted.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All users of the LSRP system are assigned privacy and security awareness training on an annual basis. The training is conducted through the VA TMS system that tracks and monitors students training records. Training is setup to test students understanding of VA policy and procedures regarding use and handling of PHI and PII information.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*

2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

This document is part of the ATO submission package; however a current 90-day ATO-C exists for the system Dated 06 January 2021.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Privacy Officers

The Privacy Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Diana L Bowen 166536

Digitally signed by Diana L Bowen 166536
Date: 2021.04.20 12:42:08 -04'00'

Privacy Officer

Signature of Information Security Systems Officers

The Information Security Systems Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Craig J. Heitz 564885 Digitally signed by Craig J. Heitz 564885
Date: 2021.04.14 17:21:55 -05'00'

Information Security Systems Officer

Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

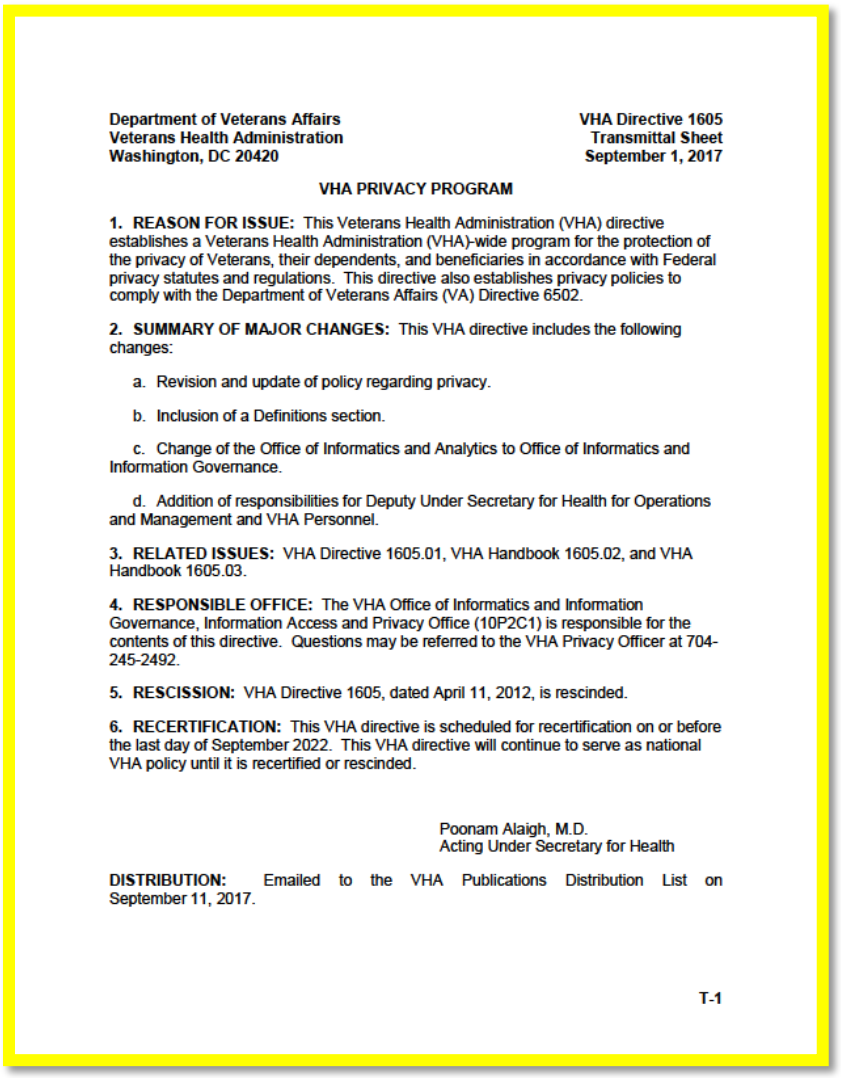
Christopher Brown
101386

Digitally signed by Christopher Brown
101386
Date: 2021.04.12 15:18:30 -05'00'

System Owner

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).



Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

VHA Directive 1605
Transmittal Sheet
September 1, 2017

VHA PRIVACY PROGRAM

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes a Veterans Health Administration (VHA)-wide program for the protection of the privacy of Veterans, their dependents, and beneficiaries in accordance with Federal privacy statutes and regulations. This directive also establishes privacy policies to comply with the Department of Veterans Affairs (VA) Directive 6502.

2. SUMMARY OF MAJOR CHANGES: This VHA directive includes the following changes:

a. Revision and update of policy regarding privacy.

b. Inclusion of a Definitions section.

c. Change of the Office of Informatics and Analytics to Office of Informatics and Information Governance.

d. Addition of responsibilities for Deputy Under Secretary for Health for Operations and Management and VHA Personnel.

3. RELATED ISSUES: VHA Directive 1605.01, VHA Handbook 1605.02, and VHA Handbook 1605.03.

4. RESPONSIBLE OFFICE: The VHA Office of Informatics and Information Governance, Information Access and Privacy Office (10P2C1) is responsible for the contents of this directive. Questions may be referred to the VHA Privacy Officer at 704-245-2492.

5. RESCISSION: VHA Directive 1605, dated April 11, 2012, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last day of September 2022. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

Poonam Alaigh, M.D.
Acting Under Secretary for Health

DISTRIBUTION: Emailed to the VHA Publications Distribution List on September 11, 2017.

T-1