



Privacy Impact Assessment for the VA IT System called:

(DSS) CyberREN

Veterans Health Administration

VISN 4 Clinical Informatics

eMASS ID: 1068

Date PIA submitted for review:

04-28-2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jeffrey Adamson	Jeffrey.Adamson@va.gov	412-822-3324
Information System Security Officer (ISSO)	Richard Alomar- Loubriel	Richard.Alomar- Loubriel@va.gov	787-696-4091
Information System Owner	Anna Crouse	Anna.Crouse@va.gov	717-269-5284

Abstract

The abstract provides the simplest explanation for “what does the system do for VA?”.

CyberREN is a renal patient care information management system, with features that address the broad range of functionality required by clinics and hospitals engaged in the treatment of all phases of kidney disease. CyberREN is used by health care professionals in all disciplines providing care for chronic kidney disease, renal replacement therapy, and kidney transplantation patients. CyberREN uses a Microsoft Structured Query Language (SQL) Server database to store data. This technology uses Thin Client, tablet, or browser-based systems to graphically present information at the point of care (POC). CyberREN communicates with Veterans Health Information Systems and Technology Architecture (VistA) using a Health Level 7 (HL7) feed through Integration Framework (DSIHW). Information is entered into CyberREN by the dialysis user, then that information is sent back to VistA/Computerized Patient Record System (CPRS) to create notes, lab orders, lab results, pharmacy orders, progress notes. Dialysis users are able to see patient information in CyberREN due to HL7 messages communicating the patient's demographics, labs, meds, problem list, diagnoses, etc. from VistA/CPRS. Patient information is also stored in the CyberREN database, which is always in the VA network, to be used for reporting, etc. Any access to the database containing the medical record is protected at the database authorization security level.

Overview

The overview is the most important section of the Privacy Impact Assessment (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:

1 General Description

- A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

CyberREN is a comprehensive medical record which addresses all the clinical documentation needs in the treatment of kidney disease. Clinical documentation modules for all phases of kidney disease are available, including hemodialysis treatment, peritoneal dialysis treatment, and chronic kidney disease as well as transplant follow-up. Clinicians delivering patient care, including physicians, nurses, patient care technicians as well as social workers and dietitians will consult and enter clinical data into the CyberREN medical record directly, i.e. at the point of care.

- B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

CyberREN is a VA Owned and VA Operated Information System

2. Information Collection and Sharing

- C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

Veterans receiving clinical treatment including hemodialysis treatment, peritoneal dialysis treatment, and chronic kidney disease as well as transplant follow-up. The expected number of individuals whose information is stored in the system varies amongst each VA facility.

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input checked="" type="checkbox"/>	Clinical Trainees
<input type="checkbox"/>	VA Contractors
<input type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

- D. *What is a general description of the information in the IT system and the purpose for collecting this information?*

Patient Information and clinical data for Nephrology

- E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The CyberREN system will be integrated with Veteran's Health Information Systems and Technology Architecture (VistA) using the Decision Support System (DSS) integration toolkit and overall Integration Framework. With two major modules for Hemodialysis and Chronic Kidney Disease, and other modules available - the solution will enable providers to deliver the best possible renal care for Veterans.

- F. *Are the modules/subsystems only applicable if information is shared?*

CyberREN is integrated with VistA. There are no subsystems.

- G. *Is the system operated in more than one site to include primary and secondary 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?*

CyberREN is operated independently at 4 primary sites in VISN 4 which are Pittsburgh, Philadelphia, Wilkes-Barre, and Wilmington.

3. *Legal Authority and System of Record Notices (SORN)*

- H. *What is the citation of the legal authority?*

5 USC 552a The Privacy Act of 1974
38 USC 501
38 USC 501(b) and 304
38 USC 7301(a)

- I. *What is the SORN?*

SORN 24VA10A7, SORN 79VA10, SORN 121VA10

- J. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No

4. *System Changes*

- K. *Will the business processes change due to the information collection and sharing?*

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

- L. *Will the technology changes impact information collection and sharing?*

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

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.

Version date: October 1, 2024

Page 4 of 39

1.1 Information 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.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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:

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Financial Information | Number (ICN) |
| <input checked="" type="checkbox"/> Full Social Security Number | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input checked="" type="checkbox"/> Military History/Service Connection |
| <input type="checkbox"/> Partial Social Security Number | Account Numbers | <input checked="" type="checkbox"/> Next of Kin |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Certificate/License Numbers ¹ | <input type="checkbox"/> Date of Death |
| <input checked="" type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Business Email Address |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input checked="" type="checkbox"/> Internet Protocol (IP) Address Numbers | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input checked="" type="checkbox"/> Medications | <input checked="" type="checkbox"/> Other Data Elements (List Below) |
| <input checked="" type="checkbox"/> Personal Fax Number | <input checked="" type="checkbox"/> Medical Records | |
| <input checked="" type="checkbox"/> Personal Email Address | <input checked="" type="checkbox"/> Race/Ethnicity | |
| <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a Different Individual) | <input type="checkbox"/> Tax Identification Number | |
| | <input checked="" type="checkbox"/> Medical Record Number | |
| | <input checked="" type="checkbox"/> Sex | |
| | <input checked="" type="checkbox"/> Integrated Control | |

Other PII/PHI data elements:

Electronic Protected Health Information (ePHI)
Service-Connected Disabilities
Employment Information
Veteran Dependent Information
Education Information
Disclosure Requestor Information

¹ *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Religious Affiliation

1.2 List the sources of the information in the system

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?

Veterans, Clinicians, VHA

1.2b 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 indicate why the system is using this source of data.

The system is used for patient care information management at the VHA.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The system creates reports for clinical use and calculates relevant scores. These reports are stored in the patient health record for clinical use.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a 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 technologies used in the storage or transmission of information in identifiable form?

Information is collected directly from patients.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is collected using paper forms (such as the enrollment form for VA health care, VAF 10-10EZ (OMB#2900-0091), VAF 10-10EZR (OMB#2900-0091), VAF 10-5345 (not subject to the paper reduction act), VAF 10-5345a (not subject to the paper reduction act), or interviews and assessments with the individual.

There are many VA forms used by Veterans to apply for medical benefits. All such VHA benefit forms are located at <http://www.va.gov/vaforms/>. The URL of the associated privacy statement is: <http://www.va.gov/privacy/>. VHA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits and/or provide specific services.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a 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.

Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary. Patient demographic information as well as income verification matching information is completed by automated tools with connections to the Austin Automation Center. Practitioners review and sign all treatment information. Various staff review data obtained and Health Information Management staff assist with corrections.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, the system does not check for accuracy by accessing a commercial aggregator of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

VA Healthcare-VISN 4 (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) systems operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veteran's Benefits, Title 38, U.S.C., Chapter 73, § 7301(b).

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191(Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009),

codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. Executive Order 9397 gives authority to collect and use the SSN as an identifier.

Privacy Act System of Records Routine Uses in Patient Medical Record – VA
24VA10P2

1.6 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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*

This 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: Risks include data breach resulting in possible identity theft, loss or corruption of data, loss of confidence in the organization. VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) systems, inclusive of information collected in the CyberREN system, contains sensitive personal information – including social security numbers, names, and protected health information - on veterans. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or if the data was otherwise breached, serious harm or even identity theft may result.

Mitigation: Veterans Health Administration (VHA), VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington), deploys extensive security measures to protect the information from inappropriate use and/or disclosure. This is done by means of both access controls and training of all employees. VA Healthcare -VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) systems security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data

minimization and retention, individual participation and redress, transparency, and use limitation. The users of the information are provided Privacy, HIPAA, and Rules of Behavior training on an annual basis. Each facility has a Chief Information Officer, Information Security Officer, and Privacy Officer on staff to assist and monitor in protecting the individual's information. Users of the information are only given access to electronic and paper documents that are needed to complete their duty tasks.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the veteran or employee	Not used
Full Social Security Number	Used as official patient/employee identifier	Not used
Date of Birth	Used to identify the veteran or employee and determine age of patient	Not used
Mother's Maiden Name	Used to identify the veteran or employee	Not used
Personal Mailing Address	Used to for communication, billing purposes and calculate travel	Not used
Personal Phone Number(s)	Used for communication, confirmation of appointments and conduct telehealth appointments.	Not used
Personal Fax Number	Used to send forms of communication and records to business contacts, insurance companies and health care providers.	Not used
Personal Email Address	Used for communication and myHealthvet secure communications.	Not used
Emergency Contact Information (Name, Phone	Used in cases of emergent situations such as medical emergencies.	Not used

Number, etc. of a Different Information)		
Financial Information	Used to calculate co-payments and VA health care benefit eligibility.	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used to communicate and bill third party health care plans.	Not used
Certificate/License Numbers	Used to track and verify legal authority to practice medicine and licensure for health care workers in a particular area of expertise.	Not used
Internet Protocol (IP) Address Numbers	Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology system to another.	Not used
Medications	Used within the medical records for health care purposes/treatment, prescribing medications, and allergy interactions.	Not used
Medical Records	Used for continuity of care	Not used
Race/Ethnicity	Used for patient demographic information and for indicators of ethnicity-related diseases.	Not used
Medical Record Number	Used as official patient identifier	Not used
Sex	Used as patient demographic identity, indicator for type of medical care or provider, and to determine the type of medical tests required for an individual	Not used
Integrated Control Number (ICN)	Used as a unique identifier used in certain systems to track and manage multiple components within a complex process or system	Not used
Military History/Service Connection	Used to evaluate medical conditions that could be related to location of military time served and to determine VA healthcare eligibility and treatment	Not used

Next of Kin	Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.	Not used
Electronic Protected Health Information (ePHI)	Used for history of health care treatment during treatment and planning of treatment	Not used
Service-Connected Disabilities	Used to determine VA health care eligibility and treatment plans/programs.	Not used
Employment Information	Used to determine VA employment eligibility, Veteran contact, and financial verification	Not used
Veteran Dependent Information	Used to determine benefit support and emergency contact person	Not used
Education Information	Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials.	Not used
Disclosure Requestor Information	Used to track and account for patient medical records released to requestors	Not used
Religious Affiliation	Use to identify clerical support for patients and staff members alike	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a 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?

The VA Healthcare-VISN 4 (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) Medical Centers systems, inclusive of information collected in the CyberREN system, uses statistics

and analysis to create general reports that provide the VA a better understanding of patient care and needs.

2.2b 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.

These reports are used by the staff and management to identify, track, and trend performance in a variety of areas including access, patient satisfaction, financial indicators, and many others. This data is never placed into the record of any patients, but is often saved as part of staff performance such as:

- The number of patients enrolled, provider capacity, staffing ratios, patient wait times, etc.
- Beneficiary travel summary/benefits
- Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

CyberREN communicates with Veterans Health Information Systems and Technology Architecture (VistA) using a Health Level 7 (HL7) feed through Integration Framework (DSIHW). Information is entered into CyberREN by the dialysis user, then that information is sent back to VistA/Computerized Patient Record System (CPRS) to create notes, lab orders, lab results, pharmacy orders, progress notes. Dialysis users are able to see patient information in CyberREN due to HL7 messages communicating the patient's demographics, labs, meds, problem list, diagnoses, etc. from VistA/CPRS. This data point, along with the entirety of the CyberREN database, is FIPS 140-2 compliant.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

SSNs are only available to certain users and are only available in configuration tables. CyberREN stores the patient's SSN in a single data point within the Patient Demographics section of the application. CyberREN application does not display the SSN to the user. The CyberREN is encrypted FIPS 140-2

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

VHA complies with OMB Memorandum M-06-15 to safeguard PII/PHI.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

Access is determined by use of the Electronic Computer Access Request, ECAR, system where program managers submit requests to Office of Information Technology (OI&T) for certain menu options based on the needs of their specific jobs or duties.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

In addition to the mandatory agency Privacy Awareness and Information Security and Rules of Behavior training for any VA employee with Network access, VHA mandates its Privacy and HIPAA Focused training for all employees who have access to PHI or VHA records, including IT systems. This training must be taken on an annual basis and completed prior to the one-year anniversary date of the previous year's training. Documentation is located at the facility where clinical technology is in use.

2.4c Does access require manager approval?

Yes.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The controls are in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of accessions of sensitive information; and formal rounds during which there is personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

Disciplinary policies are in place to address unauthorized and unapproved use of data and include the most appropriate of the following: re-training, re-education, removal of access privileges, counselling, admonishment, reprimand, suspension, and removal.

VA employees are required to report any potential privacy violations or breeches to their Information Security Officer (ISO) and Privacy Officer, and these reports are processed pursuant to VA Handbook 6500.2, Management of Security and Privacy Incidents. In addition, pursuant to the Privacy Act, the Department will review annually, the circumstances and actions of VA employees that resulted in VA being found civilly liable under Section (i) of the Privacy Act. Privacy Act, or an employee found criminally liable under the provisions of Section (i) of the Privacy Act. The purpose of this review is to determine the problem and find the most effective way to prevent recurrence.

VHA Privacy Compliance Assurance (PCA) monitors and audits compliance with privacy controls and VHA privacy policy on an ongoing basis through various mechanisms. PCA conducts virtual audits of privacy compliance of 5-7 VHA Health Care facilities annually. PCA requires an annual Facility Self-Assessment (FSA) by all VHA Health Care facilities on privacy compliance that is broken down into quarterly submissions.

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*

Name
Full 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
Financial Information
Health Insurance Beneficiary Numbers Account Numbers
Certificate/License Numbers
Internet Protocol (IP) Address Numbers
Medications
Medical Records
Race/Ethnicity
Medical Record Number
Sex
Integrated Control Number (ICN)
Military History/Service Connection
Next of Kin
Electronic Protected Health Information (ePHI)
Service-Connected Disabilities
Employment Information
Veteran Dependent Information
Education Information
Disclosure Requestor Information
Religious Affiliation

VA Healthcare VISN 4 Medical Center (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) follows national VA policies and records control schedules regarding information retention. The records include information concerning patients.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule <https://www.archives.gov/records-mgmt/grs>? This question is related to privacy control DM-2, Data Retention and Disposal.

The VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) will maintain VA data and records per the Department of Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS) 10-1 and OIT RCS 005-1.

All information collected, stored, and used for healthcare and historical information follows the Record Control Schedule (RCS) 10-1 for VHA and (RCS) 005-1 for Office of Information and Technology retention guidelines, except for, temporary files. Temporary files, also known as working papers, are documents used to make the electronic entries of information or used to temporarily and destroyed when no longer needed by the user.

Medical records are retained for 75 years after the last date of activity. Personnel, administrative, and business records are retained for various amounts of time. The guidance for retention of records is found in the Department of Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS 10-1) and the National Archives and Records Administration.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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. Please work with the system VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

3.3b Please indicate each records retention schedule, series, and disposition authority?

Medical Records Folder File or CHR: The Consolidated Health Record contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>)

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory 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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), www.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

Paper records are either shredded by an employee using an on-site VA shredder that is compliant with VA Directive 6371 www.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2 or are shredded by a contractor with Certificates of Destruction provided and destruction methods are NAID compliant.

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. 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. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1.

Information within the CyberREN system is destroyed by the disposition guidance of the RCS 10-1; maintain records for 75 years. On or before that time, VHA Records Management and Office of Information Technology will develop a plan for disposal or deletion. The plan will be routed for approval and implementations through VHA, Veterans Administration Central Office and the National Archives.

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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

All Research proposals are required to be reviewed and approved by the Facility Privacy Officer and Information Security Officer. Only the minimum necessary may be collected and used. Each protocol requires either a HIPAA Waiver, a HIPAA Authorization, or both. In addition, a Limited Data Set may be used only if the affected agencies enter into a Data Use Agreement. All research data collected for use must be in compliance with local policy and VA Handbook 1200.05, Research Activities. This includes testing.

Information used solely for training purposes must not contain patient identification. The VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) have test patients (not actual patients) that may be used for the purpose of testing and education. Any presentations that contain information based on patients must be routed through the Facility Privacy Officer to ensure all 18 HIPAA identifiers have been removed.

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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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 information retained could be subject to breach, loss, or unintentional destruction from external, internal, and physical risks.

Mitigation: The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed in accordance with the VA Records Control Schedule RCS 10-1. When the retention data is reached for a record, the medical center carefully disposes of the data by the methods described in question 3.4. The Privacy Officer, Information Security Officer, and Chief Information Officer also monitor controls to mitigate any breaches of security and privacy.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a DSS CyberREN consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DSS CyberREN and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application	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
--	---	---	---------------------------------	--	------------

Version date: October 1, 2024

Page 18 of 39

Program Interface (API etc.) that contains PII/PHI					
CyberREN Database	Yes	Yes	<ul style="list-style-type: none"> •Name • Full Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Account Information • Health Insurance Beneficiary Numbers Account Numbers • Internet Protocol (IP) Address Numbers • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Sex • Integrated Control Number (INC) • Military History/Service Connection • Next of Kin • Electronic Protected Health 	Clinical Use	The system exchanges information with VistA on the VA controlled internal network using HL7. The system does not utilize any external network communications.

			Information (ePHI) <ul style="list-style-type: none"> • Service-Connected Disabilities • Employment Information • Veteran Dependent Information • Education Information • Disclosure Requestor Information • Religious Affiliation 		
VistA Database	Yes	Yes	<ul style="list-style-type: none"> • Name • Full Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Account Information • Health Insurance Beneficiary Numbers Account Numbers • Internet Protocol (IP) Address Numbers • Medications • Medical Records • Race/Ethnicity 	Clinical Use	The system exchanges information with VistA on the VA controlled internal network using HL7. The system does not utilize any external network communications.

			<ul style="list-style-type: none"> • Medical Record Number • Sex • Integrated Control Number (INC) • Military History/Service Connection • Next of Kin • Electronic Protected Health Information (ePHI) • Service-Connected Disabilities • Employment Information • Veteran Dependent Information • Education Information • Disclosure Requestor Information • Religious Affiliation 		
--	--	--	--	--	--

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

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

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Veterans Health Information Systems and Technology Architecture (VistA)	Electronic Health Record (EHR) system used by the Veterans Health Administration (VHA) of the U.S. Department of Veterans Affairs	<ul style="list-style-type: none"> • Name • Full Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Account Information • Health Insurance Beneficiary Numbers • Account Numbers • Internet Protocol (IP) Address Numbers • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Sex • Integrated Control Number (INC) • Military History/Service Connection • Next of Kin • Electronic Protected Health Information (ePHI) • Service-Connected Disabilities • Employment Information 	<ul style="list-style-type: none"> • Electronically pulled from VistA through Computerized Patient Record System (CPRS) • CyberREN communicates with Veterans Health Information Systems and Technology Architecture (VistA) using a Health Level 7 (HL7) • CyberREN stores the patient's SSN in a single data point within the Patient Demographics section of the application. • CyberREN application does not display the SSN to the user. • CyberREN is encrypted FIPS 140-2

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		<ul style="list-style-type: none"> • Veteran Dependent Information • Education Information • Disclosure Requestor Information • Religious Affiliation 	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at VHA and VISN 4 facilities. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

The Electronic Computer Access Request (ECAR) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

Microsoft Outlook is also another tool that is used to share internal information within the organization. Risks are mitigated by using encryption methods to share sensitive information within the organization.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

<i>List IT System or External Program Office information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Version date: October 1, 2024

Page 24 of 39

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.

If no External Sharing listed on the table above, (State there is no external sharing in both the risk and mitigation fields).

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: The CyberREN system does not share information with external systems.

Mitigation: The CyberREN system does not share information with external systems.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are 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.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) provides notice of information collection in several ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual.

Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(1)(B)(iii), the

Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online:

24VA10A7, Patient Medical Records-VA (June 6, 2020)

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (November 10, 2020)

121VA10, National Patient Databases-VA (March 6, 2023)

6.1b If notice was not provided, explain why.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

VHA complies with all aspects of the Privacy Act when providing notice to patients receiving clinical care about collection, purpose, and use of sensitive patient information.

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.

Yes, individuals do have an opportunity to decline to provide information at any time, however, the VHA may not be able to enroll the Veteran. There is no penalty for declining information. The Notice of Privacy Practices states that the Veteran has the right to request a restriction of the use and disclosure of information; however, under 45 CFR § 164.522(a)(1)(vi) the VHA is not required to agree to such a restriction. Employees and VA contractors are also required to provide requested information to maintain employment or contracts with the VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington).

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.

The Veteran has the right to consent to use of U.S.C. 7332 (Alcohol and Substance Abuse, HIV, and Sickle Cell Anemia) and medical records by completing the VA Form 10-5345 to

authorized third parties information. Treatment, payment, and healthcare operations will require Veteran authorization for the use of U.S.C. 7332 information. Employees may consent to specific uses of their information on VA Form 3288 for non-medical records or VA Form 10-5345 for Employee Health Records.

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. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: *This is referring to sufficient notice provided to the individual.*

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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, employees, or general public may not be aware of the collection, maintenance, and dissemination of PII/PHI through the existence of the information systems.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practices (NOPP) when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

*7.1a 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 [VA Public Access Link-Home \(efoia-host.com\)](http://www.va.gov/foia) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals follow 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).

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington). When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at <https://www.va.gov/vaforms/medical/pdf/VHA%20Form%2010-5345a%20Fill-revision.pdf>

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealthvet program, VA's online personal health record. More information about MyHealthvet at <https://www.myhealth.va.gov/index.html>.

In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at http://www.rms.oit.va.gov/sor_records.asp.

7.1b 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)?

The system is not exempt from the access provisions of the Privacy Act.

7.1c 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?

Individuals follow 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).

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington). When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at <https://www.va.gov/vaforms/medical/pdf/VHA%20Form%2010-5345a%20Fill-revision.pdf>

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealthvet program, VA's online personal health record. More information about MyHealthvet at <https://www.myhealth.va.gov/index.html>.

In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at http://www.rms.oit.va.gov/sor_records.asp.

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.

The Veteran should provide a written request, with signature, for correcting inaccurate or erroneous information to the Privacy Officer by writing to: Privacy Office, VISN 4 1010 Delafield Rd., Pittsburgh, PA 15215, or by calling 412-822-3314 and 412-822-3324. The Privacy Officer will route the request for the correction of inaccurate or erroneous information in medical records to the author of the note. If the correction is denied by the author, the denial letter is routed to the Director's Office for concurrence and signature.

If corrections are needed for legal name, date of birth, or Social Security Number (SSN) changes, Patient Registration would process the request requiring a valid driver's license, state identification, passport, military ID, or a letter from the Social Security Administration stating the changes and a wet signature from the individual requesting the change. The Privacy Officer reviews and approves all these changes as well.

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 Notice of Privacy Practices explains the Veteran's right to request a correction to inaccurate, erroneous, untimely, or incomplete information. VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington), Community Based Outpatient Clinic (CBOC) 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. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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 to 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.** (Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

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

Principle of Individual Participation: *The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

Principle of Individual Participation: *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk of an individual not receiving notifications pertaining to appointments, medications, test results, and benefit information when the record contains incorrect information. Incorrect information documented in a record could result in improper healthcare diagnosis and treatment.

Mitigation: VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) staff verifies information in medical records and correct information identified as incorrect during each patient's medical appointments. Additionally, staff within VISN 4 are informed of the importance of maintaining compliance with VA Release of Information (ROI) policies and procedures and about the importance of remaining alert to information correction requests. An individual's identity is confirmed in requesting access, redress, and correction of information through legal authority (Power of Attorney (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. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Individuals receive access to VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) systems by employment in the VA, trainee, Without Compensation (WOC) or volunteer status, or upon being awarded a contract that requires access to our systems. An individual is assigned menu options and keys delegated by the type of access they need to complete their duty tasks. The supervisor maintains a functional category form on employees that is reviewed annually to ensure proper menu options and keys are delegated for the employee to complete duty tasks. Keys and menu options are not given if not required by the employee's duty task. Monitors and audits are completed on the functional categories by the Privacy Officers and Information Security Officers. Semi-annual reviews of computer access including CyberREN menus and keys are conducted by each service line/department through Electronic Computer Access Requests (ECAR) and approved by the Chief Information Officer (CIO) and ISO. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service, VA Police and Security Service or other security personnel.

8.1b 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?

Users from other agencies outside of VHA do not have access to the systems.

8.1c 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.

Accounts within CyberREN are configured first by discipline (Nurse, Physician, HD Technician, etc.) which sets standard read/modify/create/discard rights for chart sections which pertain to said discipline. For example, a standard HD Technician will not be able to administer medications, discard HD Orders, modify catalogues, etc.

Once default discipline rights have been applied for a user, additional rights to control what a user has read/modify/create/discard access too can be set (overriding discipline defaults). These are configured on a per-user basis by a qualified local system administrator (VA employee who is provided CyberREN Administrator Training by DSS). For example, while a standard HD Technician will not be able to modify catalogue configuration (i.e. to add new HD Machines), if a facility has a super-user HD Technician, they can be granted the ability to modify catalogues, on a per user-basis (does not impact other HD Technicians), to align with their VA roles/responsibilities.

It is up to each VA facility to configure user rights, what they can see, change, add or discard, based on their own policies and staff roles/responsibilities. Regardless of the user's discipline or custom access rights, configured by a qualified VA employee, all activities in the CyberREN system are logged for downstream auditing/compliance.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Contractors are required to complete annual Privacy Information Security, and Rules of Behavior training. Contractors having access to PHI/PII may be required to complete a Business Associate Agreement. Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Information Security, and Rules of Behavior training is completed by contractors.

8.2a. Will VA contractors have access to the system and the PII?

Contractors will only have access to the VA Healthcare-VISN 4 Medical Centers (Pittsburgh, Philadelphia, Wilkes-Barre, Wilmington) CyberREN system on a need-to-know basis in the performance of their contracted assignments/task. Access to the CyberREN system must be specified in the contract. VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete their duty task.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Yes, CyberREN has a maintenance contract in place with Document Storage Systems (DSS).

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 including employees, trainees, WOCs, volunteers and contractors are required to take annual Privacy, Information Security, and Rules of Behavior Training through the Talent Management System (TMS) course 10176 VA Privacy and Information Security Awareness and Rule of Behavior and 10203 Privacy and HIPAA Focused Training. In addition, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject-specific training on an as needed basis.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 12-03-2024
3. *The Authorization Status:* 180-DAY Authorization to Operate (ATO)
4. *The Authorization Date:* 02-07-2025
5. *The Authorization Termination Date:* 08-06-2025
6. *The Risk Review Completion Date:* 02-03-2025
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

*8.4b If not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

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. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. (Refer to question 1.8 of the PTA)

VAEC Azure Government Cloud

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (Refer to question 3.3.1 of the PTA) *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The Hosting Cloud Service Provider is the VAEC Azure Government Cloud. There is an ECSO/COMS Service Agreement for sustainment support. VHA has ownership rights over data including PII.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

VHA has ownership over the data.

9.4 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 are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, VHA is accountable for the security and privacy of the data held by a cloud provider.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

The system does not utilize Robotics Process Automation.

Section 10. 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
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Privacy Officer, Jeffrey Adamson

Information System Security Officer, Richard Alomar-Loubriel

Information System Owner, Anna Crouse

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; screen shot of a website collection privacy notice).

[The Notice of Privacy Practices](#)

[VA Form 10-5345](#)

[VA Form 3288](#)

[Notice of Privacy Practices \(NOPP\)](#)

[National Rules of Behavior](#)

[VA Handbook 6500](#)

24VA10A7, Patient Medical Records-VA (June 6, 2020)

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (November 10, 2020)

121VA10, National Patient Databases-VA (March 6, 2023)

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

<https://dvagov.sharepoint.com/sites/OITPrivacyHub>

Notice of Privacy Practice (NOPP):

VHA Directive 1605.04

[IB 10-163p \(va.gov\)](#)