Privacy Impact Assessment for the VA IT System called:

National Clozapine Registry

Veterans' Health Administration

Pharmacy Benefits Management

Date PIA submitted for review:

10/27/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Crystal White	Crystal.White@va.gov	813-972-2000x7007
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The National Clozapine Registry (NCR) is the VA's enterprise clozapine patient database. National Clozapine Coordinating Center (NCCC) staff use the NCR to track VA clozapine patients, their history of clozapine uses in the VA, and related laboratory results. It is the source of data used to prepare reports of VA clozapine prescriptions and blood test results to the Federal Drug Administration (FDA) Clozapine Risk Evaluation and Mitigation Strategy (REMS) – a legally mandated public health registry. The system contains records of the VA's clozapine patients since 1993 including patients' demographic information, FDA-required clozapine identifiers, laboratory results from each time they receive a clozapine prescription, and any clozapine pharmacy lock-out overrides that result from VA programmed safety order checks.

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

National Clozapine Registry and Pharmacy Benefits Management (PBM)

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

The National Clozapine Registry (NCR) is the VA's enterprise clozapine patient database. It is sponsored by the VHA's Pharmacy Benefits Management (PBM). The NCR's primary users and subject matter experts (SMEs) are part of the National Clozapine Coordinating Center (NCCC) which is currently a tenant of the Dallas VAMC. Clozapine is the most efficacious medication available for the treatment of schizophrenia and is the only medication proven to reduce the risk of suicide in patients with schizophrenia. Because clozapine has rare but dangerous side effects, it is subject to an FDA Risk Evaluation Management Strategy (REMS) -- a legally mandated health registry that controls use and distribution of clozapine. The NCCC is the VA's point of contact with the clozapine REMS system. The NCCC staff uses the NCR to store all information required to manage the clozapine patient treatment protocol within VA, and to report all mandatory compliance information to the FDA REMS. The NCR is necessary for the VA to provide the information required by the FDA and REMS. It is necessary for VA to retain the authority to purchase and dispense clozapine to treat schizophrenia patients.

C. Who is the owner or control of the IT system or project?

VA owned and operated.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

NCR contains information on nearly 12,000 unique clozapine patients and adds between 100 – 125 new clozapine patients a year. Records for each prescription include the name and an identifier (DEA number and/or NPI) of the over 6,400 VA providers who are registered with the NCR to prescribe clozapine within VA. The database also includes contact information with name, email, phone number for approximately 1,400 nonphysician VA employees who have communicated with the NCCC regarding clozapine treatment.

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

The National Clozapine Registry is an enterprise-wide SQL database hosted in the VA Enterprise Cloud (VAEC). The users access the NCR through a web-based application only accessible within the VA network. With its initial NCR release, there are less than 20 VA users. Subsequent NCR phase releases will allow VAMC prescribers, pharmacist, and other mental health professionals to submit clozapine requests to the NCCC through the NCR's facility dashboard. The user population may increase to 3,000 or more users. The National Clozapine Registry contains records of the VA's clozapine patients since 1993 including patient's name, social security number, demographic information, FDA-required clozapine identifiers, White Blood Cell (WBC) and Absolute Neutrophil Count (ANC) test results each time they receive a clozapine prescription as well as the identification of the prescriber, the brand of clozapine, and the daily dose.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

When a patient is registered for clozapine treatment for the first time or for subsequent registrations, the NCCC staff inputs the registration information into the database manually. When an outpatient clozapine prescription or an inpatient clozapine order is completed, the information on that patient and prescription is transmitted to the NCR via an HL7 message sent through HealthConnect using the VA Veterans Data Integration and Federation (VDIF) system. Ultimately the NCCC may use the NCR to create reports to send to the FDA via email or SFTP, but the NCR does not share data with external systems.

G. Is 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?

NCR is not currently operating in more than one site. In subsequent releases, the NCR will communicate approval of clozapine patient registration or other request to the local VAMC VistA systems via VDIF.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

SORN 24VA10A7 / 85 FR 62406 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The SORNS do not require updates and the system is not undergoing any modification.

The NCR falls under System of Record Notice SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

N/A, completing this PIA will not result in business changes. This PIA is being completed as a requirement noted in the previously approved PTA.

K. Will the completion of this PIA could potentially result in technology changes?

N/A, completing this PIA will not result in technology changes. This PIA is being completed as a requirement noted in the previously approved PTA.

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.

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:

- ☒ 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 Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

Other:

Zip Code
Lab Results
Current Medications
Primary Diagnosis
Special Conditions

- Clozapine Treatment Authorization Number
- Clozapine Treatment Authorization Status
- Clozapine Treatment Authorization
- Monitoring Frequency

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

• Prescription Number
• VistA Data File Number (DFN)

VA Employees:

• Names
• Employee facility address
• Prescriber REMS ID
• Prescriber DEA number
• National Provider Identifier

PII Mapping of Components (Servers/Database)

National Clozapine Registry (NCR) 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 National Clozapine Registry (NCR) 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 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
NCR Database	Yes	Yes, in Database table, encrypted at rest.	Name SSN DOB	Used to validate patient or employ identity to provide required information to FDA REMS.	All PII is stored in an encrypted database and transmitted via HTTPS.
NCR Database Backup, DR region	Yes	Yes, in Database table, encrypted at rest.	Name SSN DOB	Used to validate patient or employ identity to provide required information to FDA REMS.	All PII is stored in an encrypted database and transmitted via HTTPS.

1.2 What are 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?
The NCR aggregates provided clozapine data stored in facility VistA systems allowing the NCCC staff to manage clozapine treatment information and provide the required information to the FDA REMS as needed. Clozapine patients are manually added to the NCR production database, and into the virtual server residing at each facility, by the NCCC staff members entering Clozapine application/registration information.

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.

After a patient is registered, each time he or she receives a clozapine prescription, information is transmitted from the local VistA systems data files to the NCR until the NCCC manually disables authorization codes that allow prescription at the facility.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
Clozapine prescribers are manually added to NCR when the prescribers send their requests to the NCCC staff, and the individual domain enters their authority for the prescriber to use clozapine after approving their qualifications and credentials via a standard VistA permission key (YSCL Authorized key).

1.3 How is the information collected?

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?

Initial patient registration/application is submitted on a PDF form emailed to the NCCC, entered manually into the NCR, reviewed for accuracy in national EHR then enrolled officially into the FDA REMS registry via phone by NCCC personnel. Clozapine prescription information is collected from VistA files, packaged in an HL7 message that is transmitted nightly to the NCR using the VA's enterprise Health Share Health Connect server as middleware.

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?

1.4 How will the information be checked for accuracy? 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.

Clozapine data extracted from VistA will undergo data validation by the medical and administrative staff. All patients will be prescribed clozapine per diagnosis by the physician staff. However, since the FDA REMS health registry is mandated by law and requires accurate information, NCCC staff reviews the information in the national VA Electronic Health Record (EHR) to check for errors submitted on the manually inputted forms. Data that is electronically received from the VistA systems is standardized to formatting required by the FDA

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?

NCR does not use a commercial aggregator

1.5 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

Food and Drug Administration. 45 U.S.C. §164.512(b)(1)(iii): To a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA regulated product or activity.

SORN 24VA10A7 / 85 FR 62406 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

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. (*Work with your System ISSO to complete this section)*

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: NCR data could be accessed by an unauthorized person.

Mitigation: Full access to the database information is restricted by folder permissions to NCR operational personnel. Access to commands that control operations and information exchange at the facilities is also limited to those personnel. Database content, specifically that with PHI / PII, is not currently communicated outside VA and is subject to PBM release approval. Telephone communications between REMS and NCR containing PHI and PII are subject to strict HIPAA rules.

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.

The information needed by FDA REMS is designed to ensure a viable health registry and control the safe use of clozapine by tracking patients, prescribers, and pharmacies. They do this by controlling the dispensing and distribution of the medication. VA NCCC has the same business purpose, but REMS must rely on the NCCC to supply the internal controls and report the information on VA use.

PII/PHI Data Element	Internal Use	External Use
Name	File/Patient/Record Identification purposes and VDIF Support	
SSN	File/Patient/Record Identification	
DOB	File/Patient/Record Identification	
Medications	File/Patient/Record Identification	
Medical history	File/Patient/Record Identification	
Race/ethnicity	File/Patient/Record Identification	
Gender	File/Patient/Record Identification	
ICN	File/Patient/Record Identification	
Lab Results	Patient Treatment	
Current Medications	Patient Treatment	
Primary Diagnosis	Patient Treatment	
Special Conditions	Patient Treatment	
Clozapine Treatment Authorization Number	Patient Treatment	FDA Reporting
Clozapine Treatment Authorization Status	Patient Treatment	FDA Reporting
Clozapine Treatment Authorization	Patient Treatment	FDA Reporting
Monitoring Frequency	Patient Treatment	
Prescription Number	Patient Treatment	
Names	User Identification	
Employee facility address	User Identification	
Prescriber REMS ID	User Identification	
Prescriber DEA number	User Identification	
National Provider Identifier	User Identification	

2.2 What types of tools are 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?

Tools for analysis of the VA data are limited to what is available in standard VA installations, or through the resources of Pharmacy Benefits Management. Analyses concentrate on quality assurance measures to verify compliance; however, analysis of historical patient records of VA patients provides deeper insight into the causes and predictability of positive response or negative side effects.

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.

Analyses of grouped data are retained in internal reports resident in the database application. Results of analysis of individual patient information is stored in the NCCC electronic health record created for that patient. Those analyses are not directly accessible to other government employees but would be provided on specific request.

2.3 How is the information in the system 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?

The VAEC Microsoft Azure Government High protects the confidentiality and integrity of sensitive and confidential data while at rest. All sensitive and confidential data is encrypted using FIPS 140-2 compliant algorithms. The VAEC Microsoft Azure Government High system only utilizes products from the TRM that has the capability to ensure protection of information at rest. The NCR application relies on the VAEC Microsoft Azure Government High protection of information at rest.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

Upon landing on the dashboard, the only last four digits of a patient's SSN is displayed. However, when navigating to the "Patient Details" page, the full SSN is displayed. Additionally, if the user clicks on the "Patients" tab, the full SSNs for all NCR patients in the list view are displayed.

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

Each VA employee or contractor of the VA is required to undergo annual Privacy and Security training (PISA), annual HIPAA training, as well as signing the Contractor Rules of Behavior (CROB) upon initial hire.

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 to the PHI/PII in the database is limited to VA vetted personnel directly assigned to the NCR or by those assigned specifically by PBM with the following functional categories. All maintain current training to VA requirements for Privacy and Data Security.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the NCR database requires portal.azure.us. access. To obtain, user must follow standard VA processes to request and receive epas approval.

2.4c Does access require manager approval?

Yes, access to the database requires epas approval by the VA COR for users via 9957 submission and obtaining and using 0account/token to access resource.

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

Yes, access to PII is monitoring and reviewed quarterly by the Operations Manager.

2.4e Who is responsible for assuring safeguards for the PII?

The entire team (OIT, Microsoft, and Booz Allen Hamilton) would be responsible for safeguarding PII/PHI

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*

As the NCR has been identified as the primary source of information on what data has been gathered and what has been reported to FDA REMS, all data items listed in Section 1.1 have been retained in the VAEC SQL databases according to RCS 10-1 and meets VA Handbook 6500 and VHA Directive 1605.01 requirements.

1. Name
2. SSN
3. DOB.

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.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

The current NCR system inherits the FEDRAMP approved VAEC Microsoft AZURE Government Cloud (MAG) electronic records retention policy and procedures and meets VA Handbook 6500 and VHA Directive 1605.01 requirements. The NCR falls under System of Record Notice (SORN) SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA." The information is retained as defined in Records Control Schedule (RCS) 10-1 by the NCR which is the only accurate source of information on individual patient's use of clozapine within VA and subject to FOIA and OGC requests for data. When digitalizing is complete, unnecessary records will be scheduled for disposition. Paper files of patients who stopped using clozapine before 2000 but never restarted have been removed from active files but are stored in secured archive boxes within the NCCC offices in Dallas. This storage has limited access and has been reviewed by the local Health Information Management.

3.3 Has the retention schedule been 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. 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. Please work with the system Privacy Officer and 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?

A local VA Records Officer has visited NCCC and reviewed the content of the NCR records. All records meet VA and NARA guidelines. The historical records – both paper and electronic – contain elements and often actual documents of the following record schedules in various combinations. Some of these are essential to document data which is not available in the VistA record system to ensure VA compliance with FDA regulations.

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

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
Records Control Schedule 10-1
003 Administrative Management Records (GRS 16)
1004 Records Management Records (GRS 4.1)
1005 Information Services Records (GRS 14)
1006 Information Access and Protection Records (FOIA/Privacy)
1030 Ethics Program Records (GRS 25)
1150 Office of Quality and Performance
2500 Communications Records (GRS 12)
6000 Health Information Management Service
6110 Social Work Service
6400 Mental Health and Behavioral Sciences Service
7000 Medical Service
7100 Laboratory Service
7400 Pharmacy Service

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.

Elimination of electronic data is inherited from the VAEC MAG. All hardware is housed in the VAEC MAG where the NCR application and databases reside. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 30, 2019), https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8310
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 Directive 6500 in VA Publications https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&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. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents 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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

System access is controlled via Role Based Access Control (RBAC) in order to minimize the risk to privacy of using PII for research, testing or training. Users will be required to use their PIV to login to the NCR application where two factor authentication (2FA) is enabled. Access is granted by the NCR application team to those users that are approved for access and meet business need requirements. Requests for access to the data for research purposes requires submission of an PBM Data Use Agreement which is formally reviewed and approved.

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 ISSO to complete all Privacy Risk questions inside the document 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: 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: PII or PHI may be held for longer than it is required to be maintained. This extension of retention periods increases the risk that information may be breached or otherwise put at risk of access by unauthorized persons.

Mitigation: To mitigate the risk posed by information retention, when the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in Records Control Schedule 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.

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?

NOTE: Question 3.9 (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

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 PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Master Person Index (MPI)	To show what is processed by the system.	Social Security Number, Name, Date of Birth, Zip Code, Date of Death, Integrated Control Number (ICN), Data File Number (DFN)	HTTPS through REST

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

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an those who are not are not authorized which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: The privacy risk to the NCR information is minimized through various layers of security boundaries. The NCR resides in the secured VA MAG which has FIPS 140-2 encryption enabled. The VA MAG practices continuous monitoring through various tools and the overall environment is monitored by CSOC. Mitigation only occurs if information is compromised. The probability of hackers exploiting vulnerabilities is minimized and all mitigation strategies are part of CSOC SOP. The NCR application team also requests various scans of the application and mitigates any existing and open findings while working with the CSOC team.

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: 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

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 PII/PHI data elements that are processed (shared/received/transmitted)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***
FDA REMS health registry	Verification of use, safety, and VA compliance	• Patient name • SSN • Race • Ethnicity • DOB • DOD • Zip Code • Lab results	*SORN 24VA10A7 / 85 FR 62406 "Patient Medical Record-VA"* *SORN 121VA10 / 88 FR 22112 "National*	The NCCC makes an outbound call to a verified REMS

		• Medications • Primary diagnosis **Special Conditions:** • Employee names • Employee facility address • Prescriber REMS ID • Prescriber DEA number national provider identifier.	*Patient Databases-VA"*	phone number.

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.

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: There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution. A formal MOU – or what FDA REMS calls a File Interchange Agreement. NCR does not maintain summary records of interactions with REMS, however the information in each transaction is recorded on electronic documents stored in the VA database system.

Mitigation: Information provided to FDA REMS is within the scope of their authorizations. In January 2016, e-mail directly from the FDA Senior Regulatory Project Manager/ Office of Surveillance and Epidemiology Project Management Staff provided the following instructions. The Agency (FDA) has met internally and endorses the recommendation that the VA participate in the Clozapine REMS in the following ways, which has been tentatively agreed upon by the Agency, VA and Clozapine Product Manufacturers Group (CPMG):

- Enroll all prescribers in the Clozapine REMS Program.
- Enroll all patients in the Clozapine REMS Program.
- Enroll pharmacies/NCCC in the Clozapine REMS Program

• Use of the VA internal pharmacy management system to verify safe use conditions (ANC current and acceptable or have a treatment rationale, prescriber enrolled, patient enrolled) prior to dispensing clozapine prescriptions.
• Routine (at least weekly) data transfer of ANC results, treatment rationales, and pre-dispense authorization information for prescriptions dispensed at VA pharmacies in "batches" in lieu of real time to the Clozapine REMS.

Clozapine data (ANC results, treatment rationale, prescriber history) for all VA patients must be accessible to any REMS certified prescriber through both the website interface and the Clozapine REMS Call Center if a VA patient seeks care outside the VA system.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

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 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

VA does not require specific patient consent for release information to the FDA REMS health registry. The NCCC VHA Handbook recommends that the prescriber inform the patient that information will be released to the FDA as required by law to accept clozapine treatment and that refusal will in no way negatively affect their treatment by VA. The Department of Veterans Affairs does provide public notice about the information collected by the agency that is used in this system in 4 ways:

1. SORN 24VA10A7 / 85 FR 62406 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

2. SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

3. VHA Notice of Privacy Practices which are sent out every 3 years. IB 10-163 Notice of Privacy Practices, https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946, which may be used to submit requests for help.

4. This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Notice is provided.

6.1c 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.

As permitted by the authorities listed in Section 1.6, VA does not require specific patient consent for release information to the FDA REMS health registry. The NCCC VHA Handbook recommends that the prescriber inform the patient that information will be released to the FDA as required by law to accept clozapine treatment and that refusal will in no way negatively affect their treatment by VA. The Department of Veterans Affairs does provide public notice about the information collected by the agency that is used in this system in 4 ways:

1) SORN 24VA10A7 / 85 FR 62406 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

2) SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

3) VHA Notice of Privacy Practices which are sent out every 3 years. IB 10-163 Notice of Privacy Practices, https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946, which may be used to submit requests for help.

4) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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.

As permitted by the authorities listed in Section 1.6, VA does not require specific patient consent for release information to the FDA REMS health registry. The NCCC VHA Handbook recommends that the prescriber inform the patient that information will be released to the FDA as required by law to accept clozapine treatment and that refusal will in no way negatively affect their treatment by VA.

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 information gathered has a specific purpose of reporting to FDA REMS for operation of health registry relating to the patient use of clozapine. The use of the information cannot be negotiated or adjusted.

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 System ISSO 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: 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 members of the public may not know that the National Utilization Management Integration (NUMI) system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with the forms of notice discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice

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?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Nearly all the patient information gathered and reported resides in the Veteran medical record and local VistA records, therefore requests for information should be addressed to the local VA facility that recorded the information. There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at http://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from a VA medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

In the exchange between REMS and NCR, clozapine registration numbers and certain authorization codes are exchanged and recorded in the NCR database that are not available to local facility query. In that case the facility can request the information from NCR for inclusion in their records response.

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 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?

N/A. "The information in the system falls under a Privacy Act system of record and the individuals have a right of access to request a copy of the information about themselves."

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.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

If local VHA facilities do not notify the NCR of corrections the make to the information previously collected by the NCR there is not a mechanism in place to detect the changes and report them to FDA REMS. If NCR accesses the Veteran's record in the future the corrected information will be uploaded at that time.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946, which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

See Section 7.1 Additionally this would fall under VA purview.

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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: Accuracy of the individual patient demographics is dependent on the procedures of the local VA facility as well as the Master Patient Index (MPI), however errors may occur.

Mitigation: At several stages of the enrollment, SSN in the local facility records is programmatically verified to insure the correct person has been authorized and can receive clozapine. The information is verified by NCR in the EHR before reporting to FDA REMS.

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?

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?

To obtain access to NCR, users must complete the NCR New User registration form via the GUI. Users can only access this page internally within the VA. All personnel who have access to the NCR are VA employees, excepting those described in 8.2 below, who carry the functional categories assigned by their supervisor in Section 2.3 and has completed training and certification in principles of HIPAA/Privacy protections on the TMS system.

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?

All NCR users have VA PIV credentials and are not outside of the agency.

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.
NCR roles include

- Super Administrator- A user who is allowed full access to the system
- NCC Admin Staff- An advanced NCCC Staff Member with data management and admin privileges
- NCC Staff- An NCCC staff member with some functional limitations
- Viewer- Read Only Access to NCR

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, Business Associate Agreement (BAA), 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.

Yes, contractors will have access to the NCR system. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) or full BI if they will be accessing PII or PHI. Aside from the VA contractor requirements already specified in this section, contractors are not specifically required to sign additional NDAs or confidentiality agreements. Contractors are required to comply with all VA policy regarding access to systems and PII

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.

There is no additional security training for NCCC personnel over and above that required by VA. However, VA ensures that all personnel provide certificates of training annually for VA Privacy and Information Security Awareness training. All users of the MHV project team are required to sign a Rules of Behavior agreement prior to being given access to MHV systems. Additionally, the Rules of Behavior is required to be reviewed and signed annually by each user. Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS). There are two versions of the National Rules of Behavior: one for VA employees and one for contractors.

Following are the definitions of VA employee and VA Contractor:
• VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.
• VA Contractors - VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of

Behavior and complete security awareness and privacy training prior to receiving access to the information systems. Users agree to comply with all terms and conditions of the National Rules of Behavior by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 20OCT2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 16DEC2022
5. *The Authorization Termination Date:* 30NOV2024
6. *The Risk Review Completion Date:* 11OCT2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

NCR is hosted in the VAEC MAG HIGH cloud.

9.2 Does the contract with the 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 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

n/a, NCR is hosted in the VAEC MAG HIGH cloud (PAAS).

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.

n/a, NCR is hosted in the VAEC MAG HIGH cloud.

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.

n/a, NCR is hosted in the VAEC MAG HIGH cloud.

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).

n/a, NCR does not use RPA

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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.11.17 06:42:44 -08'00'

Privacy Officer, Phillip Cauthers

CRYSTAL WHITE

Digitally signed by CRYSTAL WHITE
Date: 2023.11.20 12:49:40 -05'00'

Information System Security Officer, Crystal White

DENA LISTON

Digitally signed by DENA LISTON
Date: 2023.11.20 13:28:57 -05'00'

Information System Owner, Dena Liston

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 System of Record Notice (SORN) 24VA10A7 / 85 FR 62406, "Patient Medical Record-VA"
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

The System of Record Notice (SORN) 121VA10 / 88 FR2212, "National Patient Databases-VA"
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

VA Notice of Privacy Practices (NOPP) IB 10-163:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices