Privacy Impact Assessment for the VA IT System called:

External Peer Review Program (EPRP)

Office of Informatics and Analytics

VHA

Date PIA submitted for review:

15-Mar-2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	kamilah.jackson@va.gov	513-288-6988
Information Security Officer	Gregory Fink	Gregory.fink@va.gov	304-346-9864 x124
System Owner	Nathan Gibson	Nathan.gibson@va.gov	304-346-9864 x124

Abstract

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

The External Peer Review Program (EPRP) System is designed to support a system of external review of identified medical records to assess the quality of both inpatient and outpatient care across the continuum delivered by the Veterans Health Administration (VHA) of the Department of Veterans Affairs. The External Peer Review Program (EPRP) is part of the Office of Informatics & Analytics (OI&A) and is an integral component of the VHA Medical Center, the Veterans Integrated Service Network (VISN), and the VA Central Office (VACO) Quality Management Program. The Quality Management Program is designed to measure and report various facets of health care delivery; identify and pursue opportunities for improvement in the quality of care; and establish a comprehensive database that will enable valid comparisons of VAMC and VISN specific patterns of care to the VA system as a whole, to external comparators in the private and public sector, and to support delivery of the optimal standard of care based on the most current scientific knowledge.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The External Peer Review Program VA (External Peer Review Program) EPRP System is designed to support a system of external review of identified medical records to assess the quality of both inpatient and outpatient

care delivered by the Veterans Health Administration (VHA) of the Department of Veterans Affairs. The External Peer Review Program (EPRP) is part of the Office of Informatics & Analytics (OI&A) and is an integral component of the VHA Medical Center, the Veterans Integrated Service Network (VISN), and the VA Central Office (VACO) Quality Management Program. We are not a GSS, VistA, or LAN.
The External Peer Review Program VA (External Peer Review Program) EPRP System is located at 3001 Chesterfield Avenue, Charleston, WV

The expected benefit is to expedite the processing of data associated with the External Peer Review Program Electronic Peer Review Program (EPRP) using VA workstation on the VA network within prescribed timelines via an interconnection as approved and directed by the Office of Information and Technology of The VA.

The VA_EPRP System is used to store the abstracted PHI data which is manually typed into the External Peer Review Program VA_EPRP System by External Peer Review Program EPRP reviewers while they are located on-site at
VA Veterans Health Administration (VHA) Medical Facilities and/or associated offices using VA workstations. The data is used by the off-site External Peer Review Program Data Analysis Department to deliver peer review services to VHA. External Peer Review Program will limit the volume of data exchanged with the VA to the predefined and mutually agreed upon volumes.

Approximately 700,000 individual patient medical records are stored on External Peer Review Program systems used to deliver peer review services to the VHA; however, VA will retain ownership of sensitive data transmitted to External Peer Review Program system via the interconnection.
The following requirements are applicable for VA owned sensitive information transferred via the MOU/ISA and stored on External Peer Review Program systems.

Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], Managed Services - External Peer Review Program Assessing is granted a full ATO. This ATO will expire on May 2, 2022.

The legal authority to operate this system are Title 38, United States Code, Sections 501(b) and 304

There are no circumstances that require changes to business or technology processes, and no Cloud technology or services. Data could include, but is not limited to, a variety of External Peer Review Program software for services and/or the Possibility of patient sensitive data / Electronic Patient Health Information (EPHI). EPHI data can include, but is not limited to, Patient Name, Address, Phone number, SSN, gender, Date of Birth, diagnosis, notes, and prescriptions.

The FIPS 199 sensitivity categorization is Moderate.
Confidentiality: Moderate
Integrity: Moderate
Availability: Low.

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.

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

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

Discharge/Admission Dates.

PII Mapping of Components

External Peer Review Program consists of 1 key components Database. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by External Peer Review Program and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database Server	Yes	Yes	Name, Social Security Number, DoB, Address, Phone Number, Gender, and Discharge/Admission Date	It is used to support a system of external review of identified medical records to assess the quality of both inpatient and outpatient care.	Identifiable data is not shared or transmitted outside External Peer Review Program. Stored data is encrypted.

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

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

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

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

Included within pull list from Reporting, Analytics, Performance, Improvement, and Deployment (RAPID) for the purposes of data abstraction to support the External Peer Review Program contract.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

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

The VA_EPRP System is used to store the abstracted PHI data which is manually typed into the External Peer Review Program VA_EPRP System by External Peer Review Program EPRP reviewers while they are located on-site at
VA Veterans Health Administration (VHA) Medical Facilities and/or associated offices.

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

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

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

Data elements being pulled for the EPRP review comes from an original source (CPRS/VistA) and therefore all validation of patient identifiers is done in the parent record

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

Title 38, United States Code. Sections 501(b) and 304.

24VA10A7 "Patient Medical Records-VA"
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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: 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: The FPO>VHA>QIA>External Peer Review Program system collects protected health information (PHI). Due to the highly sensitive nature of these data, there is a risk that if the data were sent via unencrypted email, serious personal, professional, or financial harm may result

Mitigation: The FPO>VHA>QIA>External Peer Review Program system employ a variety of security and privacy measures designed to ensure that the information is not inappropriately disclosed or released. These security measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

Section 2. Uses of the Information

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

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

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

To provide the VA with raw and scored data as well as reports. External Peer Review Program abstracts a subset of data already collected by the VA. Name, Social Security Number, Address, Phone number, Data of Birth, Gender, and Discharge/Admission date.

The Quality Management Program is designed to measure and report various facets of health care delivery; identify and pursue opportunities for improvement in the quality of care; and establish a comprehensive database that will enable valid comparisons of VAMC and VISN specific patterns of care to the VA system as a whole, to external comparators in the private and public sector, and to support delivery of the optimal standard of care based on the most current scientific knowledge.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly

created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Several types of analysis and scoring on the EPRP data using Analytics Software & Solutions SAS. There is the routine scoring of the measures submitted daily and the Internal Quality Control (IQC) and Internal Rate of Return (IRR) analyses.

No analysis at the individual patient level is performed.

2.3 How is the information in the system secured?

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

The External Peer Review Program information system protects the confidentiality and integrity of information at rest on laptops, desktops, servers, database servers with encryption mechanisms including full disk encryption technologies of PGP and Bitlocker.. The tracking of information at rest, and in transit, via a security risk assessment helps ensure that appropriate protections are in place to protect the confidentiality of information at rest as well as in transit.

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

Controls in place to ensure that information is handled in accordance, annual Privacy, HIPAA, and Rules of Behavior training for all employees and contractors; privacy and security briefing during new employee orientation and ongoing educational training by the Privacy Officer and Information Security Officer. Users of the information are only given controls to access the information that is essential and pertinent to complete their duty assignments

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

Access controls, audit and accountability, awareness and training, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, media protection, personnel security, physical and environmental protection, risk assessments, system and services acquisition, system and communication protection, system and information integrity, planning, and maintenance are used to meet the requirements of OMB Memoranda M-06-15 and M-06-1

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

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

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

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

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

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

Controls in place to ensure that information is handled in accordance with the uses described above include annual Privacy, HIPAA, and Rules of Behavior training for all employees and contractors; privacy and security briefing during new employee orientation, and ongoing educational training by the Privacy Officer and Information Security Officer. Users of the information are only given controls to access the information that is essential and pertinent to complete their duty assignments.
Any violations of access or use of the information are investigated by the Information Security Officer and referred to the supervisor and human resources for disciplinary action.

The External Peer Review Program information systems restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The External Peer Review Program Cisco Access Control Server and Cyber Solutions Token PIV SecurID restricts access to networking devices (routers, switches, firewalls) and privileged functions within those devices to explicitly authorized personnel. Also, access to networking devices (routers, switches, firewalls) is restricted to the local area network and by internal IP addresses in the case of the ASA5520. Server\Workstation privileged functions are limited by Active Directory. All unauthorized access is monitored by the device and GFI Software S.A. GFI for review by authorized personal. Documented in External Peer Review Program Policy IT-19.0

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

EPRP abstracts a subset of data already collected by the VA. Name, Social Security Number, Address, Phone number, Data of Birth, Gender, and Discharge/Admission date.

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?

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

According to the BAA data will be returned or destroyed upon completion of the applicable contract or agreement. Only for as long as necessary and relevant to fulfill the specified contract.
7100.12 Quality Management Records
RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

Yes. Data will be returned or destroyed upon completion of the applicable contract or agreement as approved by the Project Officer

3.4 What are the procedures for the elimination of SPI?

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

Procedures include the wiping of any media that contains PHI or PII and properly disposed of using data destruction services in accordance with VA 6500. Data destruction procedures are outlined in the Infrastructure Operations Manual in accordance with VA Directive 6500 - Media Sanitization Guideline and NIST 800-88 Media Sanitization

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

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

Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN) are utilized.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

<u>Principle of Minimization:</u> 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?

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

Follow the format below:

Privacy Risk: The risk to maintaining data within the Managed Services>FPO>VHA>QIA>External Peer Review Program system is the longer time frame that information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation: Data retention procedures are enforced through strict physical and logical access controls that include limited physical access to any VA system, complete inventory of all systems, and auditing of system or file status to ensure changes to a system status, (i.e. going offline for destruction, removal of file being wiped) is enforced by notifying appropriate personnel as well as maintained for auditing and establishing a timeline of events.

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***
Reporting, Analytics, Performance, Improvement, and Deployment (RAPID)	Quality Improvement	Name, SSN, Address, DOB, Phone Number, Gender Admission/Discharge Data	Site-to Site VPN Connection, and Public Key Infrastructures

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: There is risk that could occur due to theft or destruction.

Mitigation: Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN) are utilized.

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***
NA	NA	NA	NA	NA

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: External Peer Review Program does not share with any external organizations.

Mitigation: External Peer Review Program does not share with any external organizations.

Section 6. Notice

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

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

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

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

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

EPRP abstracts data that has already been collected by the VA and that the individuals consented to that use when it was first collected.

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis

https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false

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

EPRP abstracts data from information systems that has already been collected by the VA and that the individuals (Veterans) consented to that use when it was first collected.
Additionally, the NOPP outlines instances when VA may use their information without their consent as captured at the point of care.

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 NOPP outlines instances when VA may use an individual's information without their consent as captured at the point of care. The NOPP also addresses the individual's right to request a restriction.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that individuals are unaware that their information is being collected and that they may not have a received a copy of the NOPP.

Mitigation:

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits. 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 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

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

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

VHA has a documented process for individuals to request inaccurate, incomplete, untimely, or irrelevant PHI/PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VHA Directive 1605.01 Privacy and Release of Information. 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 SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

Individuals also have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing.

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 Notice of Privacy Practice (NOPP) 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:

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

Information can also be obtained by contacting the facility ROI office or facility Privacy Officer.

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

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

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

The VA offers a formal redress process via the amendment process is available to all individuals. The Privacy Officer provides appeal rights to the Office of General Counsel via the written response to the individual regarding the outcome of the amendment request.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:
Privacy Risk: The External Peer Review Program information system uses information already captured within the health record. There is no direct risk to an individual or their healthcare. There is a risk that an individual may not know how to request corrections to their records.

Mitigation: The VA mitigates the risk of incorrect information in an individual's records by authenticating information when possible by verifying information in medical records and corrects information identified as incorrect during each patient's medical appointments.

VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features.

In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

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

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

The External Peer Review Program information systems restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The External Peer Review Program Cisco Access Control Server and RSA SecurID restricts access to networking devices (routers, switches, firewalls) and privileged functions within those devices to explicitly authorized personnel. Also, access to networking devices (routers, switches, firewalls) is restricted to the local area network and by internal IP addresses in the case of the ASA5520. Server\Workstation privileged functions are limited by Active Directory. All unauthorized access is monitored by the device and GFI for review by authorized personal. Documented in External Peer Review Program Policy IT-19.0

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.

External Peer Review Program is a contractor for the VA. Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA Privacy Training as well as the appropriate background investigation to include fingerprinting is required. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question.

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.

In addition to the VA Privacy and Security training. External Peer Review Program policy outlines the framework to ensure that all employees have been trained in and understand the security policies and procedures. In addition, all employees will be trained on how to identify, report, and prevent potential security incidents.

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

If Yes, provide:

1. *The Security Plan Status,* ***Approved***
2. *The Security Plan Status Date,* ***24-Mar-2022***
3. *The Authorization Status,* ***Authorization to Operate (ATO***
4. *The Authorization Date,* ***November 8, 2021***
5. *The Authorization Termination Date,* ***02-May-2022***
6. *The Risk Review Completion Date,* ***02-Nov-2021***
7. *The FIPS 199 classification of the system (****MODERATE/MODERATE/LOW****).*

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

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

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).

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.

Yes. Microsoft Azure IaaS for disaster recovery. No actual work performed in cloud at this time. Enterprise Agreement directly with Microsoft Azure Government who is FedRAMP authorized.
Federal Risk and Authorization Management Program (FedRAMP) - Azure Compliance | Microsoft Docs >>

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)

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

Yes External Peer Review Program has ownership.
Confidentiality.
"Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including Customer Data, Professional Services Data, and the terms of Microsoft Agreements. The Online Services Terms may provide additional obligations for, and limitations on disclosure and use of, Customer Data. Confidential Information does not include information that (1) becomes publicly available without a breach of this agreement, (2) the receiving party received lawfully from another source without a confidentiality obligation, (3) is independently developed, or (4) is a comment or suggestion volunteered about the other party's business, products or services. Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose that Confidential Information to third parties, except to its employees, Affiliates, contractors, advisors and consultants ("Representatives") and then only on a need-to-know basis under nondisclosure obligations at least as protective as this agreement. Each party remains responsible for the use of Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party.
A party may disclose the other's Confidential Information if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.
Neither party is required to restrict work assignments of its representatives who have had access to Confidential Information. Each party agrees that the use of information retained in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this agreement or trade secret law, and each party agrees to limit what it discloses to the other accordingly.
These obligations apply (1) for Customer Data until it is deleted from the Online Services, and (2) for all other Confidential Information, for a period of five years after a party receives the Confidential Information.
X20-10009, X20-10137, X20-12586, SCE41,SCE21, 1092393.002, X20-12875, X20-12803

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.

Yes, The CSP collects metered data and consumption of resources. Only for External Peer Review Program review.

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. Although FedRAMP authorized, External Peer Review Program must further implement NIST 800-53, etc, security and privacy to meet those requirements within the External Peer Review Program environment.

Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose that Confidential Information to third parties, except to its employees, Affiliates, contractors, advisors and consultants ("Representatives") and then only on a need-to-know basis under nondisclosure obligations at least as protective as this agreement. Each party remains responsible for the use of the Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party. A party may disclose the other's Confidential Information if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.

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).

Not applicable

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**

ID	Privacy Controls
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.

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.05.11 08:58:29 -04'00'

Privacy Officer, Kamilah Jackson

Digitally signed by Gregory B. Fink 1561196 (affiliate)
Date: 2022.05.10 16:28:48 -04'00'

Information System Security Officer, Gregory Fink

Nathan Gibson

Digitally signed by Nathan Gibson
Date: 2022.05.10 16:26:01 -04'00'

Information System Owner, Nathan Gibson

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).

More information VA Privacy Service

https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false