Privacy Impact Assessment for the VA IT System called:

CAMP LEJEUNE ENVIRONMENTAL ACTION REPORT (CLEAR)

Member Services (MS), Health Eligibility Center (HEC)

Atlanta Area – eMASS # 678

Date PIA submitted for review:

5/14/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shirley Hobson	Shirley.Hobson@va.gov	629-259-3849
Privacy Officer	Angela F. Harris	Angela.Harris2@va.gov	404-548-5759
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340
Information System Owner	William Brock	william.brock@va.gov	404-321-6111 ext. 206200

Abstract

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

The Camp Lejeune Environmental Action Report (CLEAR) is tasked with collecting the names of all Veterans and family members who may have resided at Camp Lejeune that have been exposed to tainted groundwater at Camp Lejeune, North Carolina. CLEAR allows Veteran Affairs Medical Centers to collect the names of all Veterans and family members who may have resided at Camp Lejeune during the time period of 1957 – 1987. It is a mechanism to track Veterans who served on active duty at Camp Lejeune (North Carolina) and eligible family members with one or more of 15 specified illnesses or conditions in order to provide hospital care and medical care.

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?

The IT system is Camp Lejeune Environmental Action Report (CLEAR) and falls under the system boundary of Area Atlanta. The business owner is The Veterans Health Administration (VHA), Member Services (MS), and Enterprise Service Support. CLEAR is operated under the legal authorities of Public Law 112-154, 2012.

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 VHA established the Camp Lejeune Implementation (CLI) Task Force to develop and implement policy, system and process changes from an interdisciplinary team of subject matter experts from across multiple work centers within VA (VHA and Veterans Benefits Administration (VBA)). The CLI Task Force is led by two senior-level executives, currently supported by a small core team with responsibility for initiation, planning, execution, monitoring and controlling, and closeout. Six functional work stream teams were chartered and tasked with ensuring that VA infrastructures are capable and adapted - Veteran Administrative Eligibility Work Stream, Communications Work Stream, Clinical Eligibility Work Stream, Delivery of Care Work Stream, Family Member Administrative Eligibility Work Stream, Legal/Regulations Work Stream. Clear is hosted at HEC, Atlanta, GA.

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

Area Atlanta and business owner is VHA, Member Services, and Enterprise Service Support

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?

As of May 9th, 2024, 72972 individuals including Veterans and family members participate in this program.

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

CLEAR verifies Camp Lejeune residency to qualify individuals for access to treatment. CLEAR connects with Enrollment System Redesign (ESR) to query for Veteran enrollment information. It qualifies individuals for access to treatment. Veterans and family member names will be collected and submitted to the Health Eligibility Center (HEC) via HEC Alert for tracking and verification purposes. Veterans and Family Members information will be tracked in the CLEAR database. Enrollment Eligibility Division (EED) staff will verify and update CLEAR.

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

Through secure file transfer protocol, CLEAR shares PII with VA internal IT system - the Veteran Enrollment System.

G. Is the system 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?

CLEAR is only hosted in Area Atlanta HEC Data Center.

3. Legal Authority and SORN

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

CLEAR is operated under the legal authorities of Public Law 112-154, 2012 https://www.oprm.va.gov/privacy/systems_of_records.aspx.
SORN: Enrollment and Eligibility Records- VA 147-VA10

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 HEC-VHA is not in the process of modifying our system, therefore; the SORN modification will not be required at this time. The Area Atlanta does not use cloud technology at this time.

4. System Changes

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

The completion of this Privacy Impact Assessment will not result in any changes to business processes within the Health Eligibility Center.

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

The completion of this Privacy Impact Assessment will not result in any technology changes within the Health Eligibility Center.

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)

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

Other PII/PHI data elements: Service Number, Gender, branch of service, components, dates residency at Camp Lejeune, Proofs used to verify residency, reasons for denial, health conditions, relationship to Veteran.

PII Mapping of Components (Servers/Database)

CLEAR consists of two key components (servers/database and application). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **CLEAR** 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**
HECAlert/Clear Database	Yes	Yes	Name, Social Security Number (SSN), Date of Birth, Personal Mailing Address, Personal Phone number, Personal Email, Service Number, Gender, Branch of Service, Components, Dates residency at Camp Lejeune, Proofs used to verify	To register a Veteran to Camp Lejeune program.	Information System complies with NIST 800-53 requirements including database encryption and application secure code review.

			residency, Reasons for denial, Health Conditions, Relationship to Veteran		
CLEAR Web Site	Yes	Yes	Name, Social Security Number (SSN), Date of Birth, Personal Mailing Address, Personal Phone number, Personal Email, Service Number, Gender, Branch of Service, Components, Dates residency at Camp Lejeune, Proofs used to verify residency, Reasons for denial, Health Conditions, Relationship to Veteran	HEC will verify submitted information.	Information System complies with NIST 800-53 requirements including database encryption and application secure code review.

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 data is collected from the Veteran, Spouse, dependents, military service records, Registration and Eligibility system users.

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.

Data from ESR to verify Veteran enrollment status.

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

CLEAR does not produce a score, analysis or report as a source of information.

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?

Sensitive Personal Information (SPI) information is only collected directly from the Veteran or the application the Veteran completes for medical care.

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?

The information is collected directly from the Veteran, spouse or dependent. If the data is collected from the Military Service, it is done so by an Enrollment and Eligibility Division staff member when they then use Veterans Information Solution (VIS), eFolder, Military Service Data Sharing (MSDS), information from the Marines data base to verify the Veteran was stationed at Camp Lejeune during the specified dates according to this law.

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.

The SPI data is collected and stored in the CLEAR so that it can be used to match the data in the Enrollment System (ES). This data is also used to help identify the Veteran and family members that are possibly eligible for Camp Lejeune related benefits.

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?

CLEAR does not check for accuracy by accessing a commercial aggregator of information.

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

The Camp Lejeune Veterans System Changes project is being undertaken to support legislation Honoring America's Veterans and Caring for Camp Lejeune Families Act of 2012 signed on August 6, 2012 (Public Law 112-154). VA needs to provide hospital care and medical services to Veterans who served on active duty at Camp Lejeune (North Carolina) and to eligible Family Members for one or more of 15 specified illnesses or conditions. To be eligible for care under the provisions of this bill, the Veteran and/or Family Member must have resided or served on active duty at Camp Lejeune for not fewer than 30 days between January 1, 1957, and December 31, 1987.

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: There is the possibility of misinformation being provided by the individuals without validation for the sake of getting some treatment under this law that eventually may result in charges to be levied to the individual.

Mitigation: Verification of individual data across systems through seamless integration via HEC Alert for tracking and verification purposes.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the Veteran or family member.	Not used
Social Security Number	Used as a Veteran identifier and as a resource for verifying enrollment status	Not used
Date of Birth	Used to identify age and confirm Veteran identity	Not used
Mailing Address	Used for communication purposes	Not used
ZIP code	Used for communication purposes	Not used
Phone Number(s)	Used for communication purposes	Not used
Email Address	Used for communication purposes	Not used
Service Number	Used to identify Veteran	Not used
Gender	Used to identify Veteran or Family member	Not used
Branch of Service	Used for service affiliation	Not used
Components	Used for service affiliation	Not used
Dates of Residency at Camp Lejeune	Used to validate benefits eligibility	Not used
Proofs used to Verify Residency	Used to validate residency	Not used
Reason of denial	Used to validate historical claim	Not used
Health Conditions	Used to establish eligibility requirement	Not used
Relationship to Veteran	Used to establish eligibility requirement	Not used

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?

In order to fulfill the legislative requirements, the CLEAR was implemented and is in use until system changes can be fully implemented through front end applications (Registration, Enrollment, and Eligibility), point of care (Computerized Patient Record System, Scheduling, Pharmacy, etc.), and back office (Integrated Billing, Office of Policy and Planning reporting, etc.). CLEAR does not analyze the input data to create new data

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.

The data collected in CLEAR is used to identify Veterans and family members eligible for care under the Legislative changes for Camp Lejeune.

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?

Database storing WRAP data is encrypted. Users' connection to the system is encrypted using latest Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols.

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

Access to system is limited; access requires Personal Identity Verfiication (PIV) card; access to system and components is Audited.

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

Access to system is limited; access requires PIV card; access to system and components is Audited.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access is granted on a need-to-know basis. Users must take VA HIPPA Focused Training and VA Privacy and Information Security Awareness and Rules of Behavior training annually. Users' supervisors are informed as training is about to lapse via the Talent Management System (TMS).

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

Users must submit a signed VA Lightweight Electronic Action Framework (LEAF) Access Request form, obtain supervisor's signature for approval . Role, training, and approval are documented through this workflow process.

2.4c Does access require manager approval?

Users' supervisor and department manager must approve a LEAF access request before users being grant access to CLEAR.

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

Only authorized and vetted patrons are allowed access to CLEAR. CLEAR inherits information monitoring from the VA which includes auditing capabilities and generation of system audit log records minimally including: event type; time/date of event; event Location; event Source; event Outcome; identity of user / system associated with the event (e.g., username, full name, remote IP Address, remote host name, server IP address, server host name).

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

Office of Information and Technology (OIT) staff safeguards the database and servers hosting CLEAR. Business determines users access to the CLEAR.

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

Currently all information that has been entered into the database is still within that System. The information is being held pending the migration of the database into the Enrollment System itself. Information includes Name, Social Security Number (SSN), Date of Birth, Personal Mailing Address, Personal Phone number, Personal Email, Service Number, Gender, Branch of Service, Components, Dates residency at Camp Lejeune, Proofs used to verify residency, Reasons for denial, Health Conditions, Relationship to Veteran.

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.*

At present, all information will remain within the database pending migration. Currently, that migration is under review by systems management. Target date has not been set as of the reporting of this document.

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?

All records are maintained in accordance with the VA Office of Information & Technology (OI&T) NARA and General Record Schedule (GRS) 3.1 Item 51 with disposition authority of DAA-GRS-2013-0005-0003.

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

All records within the database are considered temporary as they are going to be migrated into the Enrollment System and the CLEAR Database will be rendered useless at that time.

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.
All records within this database are temporary and can be destroyed upon entry into the Enrollment System and/or other databases maintained by AITC and other OIT entities.

Per Records Disposition Process: (44 U.S.C. Chapter 33), once the legal retention requirements have been satisfied. The most appropriate method will depend on the format and security classification of the records, the methods available, and the destruction process for the records in question.

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.

Information in the CLEAR database is not used for testing or research purposes.

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 for 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: Risk of privacy breach is minimal in this situation. The information is for a limited audience nationally and very few staff have access to the information as a whole within the databases. There is a risk that the information maintained by CLEAR could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at risk of being unintentionally released or breached.

Mitigation: While the information is reported to multiple facilities within VA, access is extremely restricted to those with a need to know basis only. All information is maintained within accordance to VA, HIPPA and Federal privacy regulations.

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***
Enrollment System	Enrollment System is the authoritative source for Eligibility and Enrollment for Veterans. The data from the	Name, Social Security Number (SSN), Date of Birth, Personal Mailing Address, Personal Phone number, Personal Email, Service Number, Gender, Branch of Service, Components, Dates	Secure File Transfer

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*
	CLEAR will be used to correctly identify the Veterans that are eligible for Camp Lejeune once the Camp Lejeune software is in the Enrollment System (ES) It is currently working on the changes to ES	residency at Camp Lejeune, Proofs used to verify residency, Reasons for denial, Health Conditions, Relationship to Veteran	

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 for this section).

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

Follow the format below:

Privacy Risk: The risk with sharing data internally is that data may be disclosed to individuals who do not require access.

Mitigation: Only staff with a need to know is allowed access to the system and must complete the appropriate steps to gaining that access. Access to this system follows established VA guidelines which require the user to request access via a HEC access request which must be approved by the supervisor, the Information System Owner (ISO) and the Director of the service. Access requirements include a current Background Investigation, current VA Privacy and Information Security Awareness and Rules of Behavior and Privacy and HIPAA training, as well as approval by the supervisor certifying the employee's need to know the information.

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***
N/A	N/A	N/A	N/A	N/A

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: No external sharing

Mitigation: No external sharing

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.

CLEAR does not use personal information for secondary purposes. The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN) 172VA10, 121VA10, and 79VA10 When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

CLEAR is operated under the legal authorities of Public Law 112-154, 2012
https://www.oprm.va.gov/privacy/systems_of_records.aspx.
SORN: Enrollment and Eligibility Records- VA 147-VA10 .

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

Information collected in the CLEAR initially has been started because the Veteran or the Veteran's Family member has begun the process. The Veteran or the Veteran's Family Member has to initiate the Camp Lejeune process by identifying themselves as a Camp Lejeune Veteran or Family Member. The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary.

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.

Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the *Federal Register* and available online:

https://www.oprm.va.gov/privacy/systems_of_records.aspx.
SORN: Enrollment and Eligibility Records- VA 147-VA10

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.

The Veteran can stop the process at any time and refuse to be enrolled at the VA. If a denial letter is necessary, they are sent from the Enrollment System (ES).

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.

Individuals have the right to consent to particular uses of information. Individuals are directed to use the 10-5345 Release of Information form describing what information is to be sent out and to whom it is being sent to.

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 for 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 Veterans and other members of the public will not know that the CLEAR exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The Area Atlanta mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1

Section 7. Access, Redress, and Correction

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

7.1 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.***

There are no procedures for individuals to gain access to their information on CLEAR. Individuals who desire to gain access to their information must contact the application which originally gathered the information. (ESR)

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)?

CLEAR is not exempt from the provisions of the Privacy Act

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

CLEAR is not exempt from the provisions of the Privacy Act.

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.

There are no procedures for correcting inaccurate information. Individuals who desire to correct inaccurate information must contact the application which originally gathered the information: Enrollment System (ES)

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.

There are no procedures for correcting inaccurate information. Individuals who desire to correct inaccurate information must contact the application which originally gathered the information: Enrollment System (ES)

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.

The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to

amend or correct records, the System Owner must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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 for 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: There is a risk that a Veteran could accidentally provide incorrect information to VA when enrolling for health benefits and that incorrect information could be used to determine case status.

Mitigation: CLEAR does not directly mitigate this risk, as it uses information provided by the Enrollment System for consistency checks. All processes to enroll, determine eligibility, and update Veterans information are performed in the Enrollment System. However, Veterans do have the ability to update their enrollment information using VA form 10-10EZR.

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?

Access to this system is granted to the individual after they have completed the VA LEAF Access Request for CLEAR, signed the Security Agreement for the system, and completed the

required VA Privacy and Information Security Awareness and Rules of Behavior and Privacy and HIPAA courses. The LEAF access request must contain all of the line items on the form; contain the requestor's signature, and supervisor's approval. Once all required documentation has been received and reviewed, LEAF Access request form will be forwarded to the access group that creates the account.

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?

Not Applicable. Users from other agencies do not have access to CLEAR.

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.

There are 3 roles to the CLEAR. Administrator accounts have the rights to view and update a CLEAR record. View Only accounts have view/read only access. These users are the Active Directory (AD) Group VHA CLEAR Users group. Submitter access has the authority to submit CLEAR requests via HEC Alert site. Authorized users of CLEAR gain access using windows authentication to access the web site.

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.

OIT contractors will have access to the systems because the servers where the applications reside are hosted by OIT Area Atlanta. Access is required by the contractors for operations and maintenance but is limited by separation of duties. OIT contracts are fixed rate and do not require reviewing unless there's a need to validate contractor responsibilities or additional information is needed off the contract. If the contract has an option year, then it is reviewed prior to exercising the option. All OIT contract staff sign a Non-Disclosure Agreement, which is maintained by the Contracting Officer Representative (COR). Currently, the OIT staffing contract is reviewed quarterly by the COR.

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.

VA Privacy and Information Security Awareness and Rules of Behavior and Privacy and HIPAA courses will be completed within the Training Management System (TMS)

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* <<N/A>>
2. *The System Security Plan Status Date:* <<N/A>>
3. *The Authorization Status:* <<N/A>>
4. *The Authorization Date:* <<N/A>>
5. *The Authorization Termination Date:* <<N/A>>
6. *The Risk Review Completion Date:* <<N/A>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<N/A>>

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.***

CLEAR is a minor application currently covered under the Area Atlanta information system enclave FIPS 199 classified moderate risk Authority to Operate (ATO) signed **22 May 2022** by the Authorizing Official (AO), Dewaine Beard. This ATO expires on **21 May 2025.**

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)*

CLEAR does not use Cloud technology.

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.*

CLEAR does not use Cloud technology

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.

CLEAR does not use Cloud technology

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.

CLEAR does not use Cloud technology

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).

CLEAR 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 provided in this Privacy Impact Assessment is true and accurate.

SHIRLEY HOBSON Digitally signed by SHIRLEY HOBSON
Date: 2024.07.19 12:36:33 -05'00'

Privacy Officer, Shirley Hobson

ANGELA HARRIS Digitally signed by ANGELA HARRIS
Date: 2024.07.18 12:46:54 -04'00'

Privacy Officer, Angela F. Harris

Knight, Howard (HEC ISSO) Digitally signed by Knight, Howard (HEC ISSO)
Date: 2024.07.17 13:59:23 -04'00'

Information System Security Officer, Howard Knight

WILLIAM BROCK Digitally signed by WILLIAM BROCK
Date: 2024.08.06 07:03:52 -04'00'

Information System Owner, William Brock

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)

CLEAR is operated under the legal authorities of Public Law 112-154, 2012 https://www.oprm.va.gov/privacy/systems_of_records.aspx.

SORN: Enrollment and Eligibility Records- VA 147-VA10 .

NOPP: http://www.va.gov/vhapublications (Brochure #10-163P)

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