



Privacy Impact Assessment for the VA IT System called:

# Camp Lejeune Family Member Program (CLFMP)

## Financial Services Center (FSC) Veterans Administration (VA)

### VACO

Date PIA submitted for review:

May 16, 2022

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Princess Miller	Princess.Miller@va.gov	512-460-5148
Information System Security Officer (ISSO)	Rito-Anthony Brisbane	Rito-Anthony.Brisbane@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-981-4871

## Abstract

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

Camp Lejeune Family Member Program (CLFMP) resides at the VA Austin Information Technology Center (AITC) and the program office is in the Financial Healthcare Service, Medical Claims Division. CLFMP provides an automated medical claims processing system from receipt of medical claims documents through claims payment including the appropriate accounting transaction. The Camp Lejeune Family Member Program (CLFMP) is for family members of Veterans that lived or served at U.S. Marine Corps Base Camp Lejeune, North Carolina, between August 1, 1953, and December 31, 1987, and were potentially exposed to drinking water contaminated with industrial solvents, benzene, and other chemicals.

## 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 Camp Lejeune Family Member Program (CLFMP) resides only at the VA Austin Information Technology Center (AITC) and the program office is in the Financial Healthcare Service, Medical Claims Division. Approximately 750 family members have applied for and been granted admission to the program. Expected number of future applications for enrollment is estimated to be less than 50 per year and will decrease with time.

Personally Identifiable Information (PII) and Personal Health Information (PHI) Healthcare data is shared with Veterans Healthcare Administration Office of Community Care (VHA/OCC). This information includes personal and medical information demonstrating that they family member resided on Camp Lejeune during the affected period and that they have, as a result, incurred one or more of the medical conditions listed by the program. This PIA will not result in any business or technology change requirements.

- This program is the result of Public Law (PL) 112-154, Honoring America’s Veterans and Caring for Camp Lejeune Families Act of 2012 signed on August 6, 2012. From January 1, 1957, through December 31, 1987, people living or working at the U.S. Marine Corps Base Camp Lejeune, North Carolina, were potentially exposed to drinking water contaminated with industrial solvents, benzene, and other chemicals. PL112-154 requires the Department of Veterans Affairs (VA) to provide health care to eligible Veterans and family members. System of Records Notice SORN is clear about the use of the information, specifically 13VA047 “Individuals Submitting Invoices-Vouchers For Payment-VA”; routine use is under revision and 23VA10NB3 “Non-VA Fee Basis Records-VA.( <https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E920911.pdf> )

## Section 1. Characterization of the Information

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

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

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (<https://vawww.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:

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

- prior medical authorization number and services
- medical diagnosis codes
- Medical diagnosis
- Dates of treatment
- physician name and contact information
- Billed and Payable amounts
- Physician Name
- Physician Tax Identification Number/SSN
- Physician National Provider Identifier (NPI)
- Physician Telephone
- Physician Address
- Physician Email Address
- Patient Control Number

**PII Mapping of Components**

The Camp Lejeune Family Member Program (CLFMP) - Camp Lejeune Family member program consists of 4 key components (database). This component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CLFMP 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
PCM CampLejeune	Yes	Yes	Family Members <ul style="list-style-type: none"> <li>• Full Names</li> <li>• SSN</li> <li>• Date of Birth</li> <li>• personal addresses</li> <li>• personal email addresses</li> <li>• social security number</li> <li>• date of birth</li> <li>• personal telephone numbers</li> <li>• emergency contact information</li> <li>• healthcare insurance beneficiary account numbers</li> <li>• current medications</li> <li>• prior medical authorization number and services</li> <li>• previous medical record</li> <li>• medical diagnosis codes</li> <li>• Medical diagnosis</li> <li>• Dates of treatment</li> <li>• physician name and contact information</li> <li>• Physician Name</li> <li>• Physician Tax Identification Number/SSN</li> <li>• Physician National Provider Identifier (NPI)</li> <li>• Certificate/License Number</li> </ul>	To determine enrollment and process claims	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

			<ul style="list-style-type: none"> <li>• Physician Telephone</li> <li>• Physician Address</li> <li>• Physician Email Address</li> </ul>		
FSC DataDepot	Yes	Yes	Vendor ID/Vendor Code (SSN) Vendor Name Vendor Address Vendor Telephone TaxID (SSN)	<b>To validate vendor information</b>	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.
FSC Transaction Service	Yes	Yes	<b>Patient Control Number</b>	<b>To track claims to patients</b>	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator

					management, audit, and encrypted transmission.
<b>CLFM</b>	<b>Yes</b>	<b>Yes</b>	<ul style="list-style-type: none"> <li>• healthcare insurance beneficiary account numbers</li> <li>• current medications</li> <li>• prior medical authorization number and services</li> <li>• previous medical record</li> <li>• medical diagnosis codes</li> <li>• Medical diagnosis</li> <li>• Dates of treatment</li> <li>• physician name and contact information</li> <li>• Physician Name</li> <li>• Physician Tax Identification Number (SSN)</li> <li>• Physician National Provider Identifier (NPI)</li> <li>• Certificate/License Number</li> <li>• Physician Telephone</li> <li>• Physician Address</li> </ul>	<b>To validate medical claims and enrollment</b>	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

**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.*

- Family members as well as Power of Attorney/Proxy can provide information related to Camp Lejeune Family Member Program.
- At the completion of the claims process, an Explanation of Benefits (EOB) that explains which claims were paid or denied is sent to the patient and to the provider submitting the claim.

### **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.*

Most of the information is received via electronic transmission from another system; eligibility data from Administrative Data Repository (ADR).

Information is primarily provided by the individual. In some situations, a Power of Attorney/Proxy could provide the information.

### **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.*

Received via electronic transmission from another system; eligibility data from Administrative Data Repository (ADR). For Camp Lejeune the information is primarily provided by the individual. In some situations, a Power of Attorney/Proxy could provide the information. Information is manually validated when a family member initially applies and each time a claim is submitted. Information submitted is manually validated for accuracy prior to processing/paying the claim.

Validation is performed to validate the services identified by the service provider matches the information contained in the authorization. As part of the Camp Lejeune Family Member Program (CFLMP), there is information provided initially by the Family Member as it relates to their medical condition before they are deemed eligible to participate in (CLFMP) Validation is done to ensure the medical claims being submitted for payment are part of their specified eligibility parameters established at the time they are deemed clinically eligible for the program.

### **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*

Veterans' Benefits: Title 38, United States Code, Sections 1703, 1724, 1725, 1728, 1781, 1802, 1803, 1813, and Public Law 112-154 which amends title 38, United States Code, to furnish hospital care and medical services to veterans who were stationed at Camp Lejeune, North Carolina, while the water was contaminated at Camp Lejeune.

### **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:** Sensitive Personal Information including personal contact information, medical information, service information and benefit information may be released to unauthorized individuals.

**Mitigation:** CLFM adheres to information security requirements instituted by the VA Office of Information Technology (OIT). CLFM relies on information previously collected by the VA from the individuals. Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. The systems undergo complete Web Application Security Assessment (WASA) scans and are not allowed to operate with critical findings. The applications have improved their user validation practices and procedures to ensure user access is authorized.

## 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.*

Name: Used to identify the patient

Social Security Number: Used as a patient identifier

Date of Birth: Used to identify patient age and confirm patient identity

Mailing Address: Used to contact patient

Zip Code: Used to contact patient

Phone Number(s): Used to contact patient or provider

e-mail address: Used to contact patient or identify provider

Emergency Contact Information: Used to notify Next of Kin

Health Insurance Beneficiary Account Numbers: Used to identify the patient

Certificate/License Numbers: Used to verify the patient  
Tax Identification Number: Used to Identify the patient or provider  
Information is processed to ascertain eligibility and make medical claims benefits payments.  
Prior medical authorization number and services: Used to validate family member claim  
Medical diagnosis codes: Used to validate family member claim  
Medical diagnosis: Used to validate family member claim  
Dates of treatment: Used to validate family member claim  
Billed and Payable amounts: Used for claim processing  
Physician Name: Used for claim processing  
Physician Tax Identification Number/SSN  
Physician National Provider Identifier (NPI)  
Physician Telephone  
Physician Address: Used for claim processing  
Physician Email Address: Used for claim processing  
Account numbers Used for payment services (Financial Account Information)  
Current Medications: Used to validate family member claim  
Previous Medical Records: Used to validate family member claim  
Financial Account Information: Used for processing payments

## **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*

The limited analysis of the data is used to determine eligibility and claim payment. The system generates an Explanation of Benefits (EOB) and an Explanation of Payments (EOP) that explains which claims were paid or denied. EOBs and EOPs are sent to the patient and to the provider submitting the claim. This data is tied to the patient record as a data string.

## **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?*

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

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

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

- 2.3a protect data through encryption in transit and at rest
- 2.3b SSN's are masked to all but the VA staff providing assistance.
- 2.3c All employees and contractors are required to participate in general and role-based privacy training annually, all appropriate administrative, technical and safeguards have been implemented to protect CLFM, data accessed and displayed by the system and users of the system and these controls are reviewed regularly

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

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

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

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

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*

*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

Add answer here:

- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
- System of Records Notice (SORN) is clear about the use of the information, specifically 13VA047 “Individuals Submitting Invoices-Vouchers For Payment-VA”; routine use is under revision and 23VA10NB3 “Non-VA Fee Basis Records-VA.( <https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E920911.pdf> )
- Disciplinary actions: Depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

- The information is required to process medical claims; without this information, we would not be able to accomplish our mission. Employees requiring access to this system must sign a VA Rules of Behavior (ROB), complete automated annual privacy training and attend classroom training sessions as needed.

## Section 3. Retention of Information

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

### 3.1 What information is retained?

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

Name  
Social Security Number  
Date of Birth  
Personal Mailing Address  
Personal Phone Numbers  
Personal Email Address  
Emergency Contact Information  
Health Insurance Beneficiary Account Numbers  
Current Medications  
Previous Medical Prescriptions  
Tax ID  
Prior medical authorization number and services  
Medical diagnosis codes  
Medical diagnosis  
Dates of treatment  
Physician name and contact information  
Billed and Payable amounts  
Physician Name  
Physician Tax Identification Number/SSN  
Physician National Provider Identifier (NPI)  
Certificate/License Number  
Physician Telephone  
Physician Address  
Physician Email Address

### 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.*

Data is retained for 6 years, 3 months as required by General Record Schedule (GRS) 1.1: Accountable Officers' Accounts Records for each claim as they are recorded separately.

**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, General Record Schedule (GRS) 1.1 6: Accountable Officers' Accounts Records, which is governed by Government Accountability Office (GAO) regulations on retention of payment related records.

The retention schedule has been approved by NARA.

<https://www.archives.gov/files/records-mgmt/grs/grs06-1.pdf>

**3.4 What are the procedures for the elimination of SPI?**

*Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?*

*This question is related to privacy control DM-2, Data Retention and Disposal*

6 years 3 months as required by GRS 1.1 Item 1a. Records Officer and Records Liaison Officer comply with VA Handbook 6300.1 Chap 6, Section 3. We are also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions. Paper records are shredded by a local shredding company weekly

**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*

We do not use PII data for testing or training 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.*

*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:** If information maintained by the FSC CLFMP is be retained for longer than is necessary to fulfill the VA mission. Then, records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** CLFMP In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in FSC CLFMP is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only if necessary.

The Records Manager ensures data retention policies and procedures are followed. The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

**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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Document Management System (DMS)	Internal collection of submitted forms	<ul style="list-style-type: none"> <li>• Full Names</li> <li>• SSN</li> <li>• Date of Birth</li> <li>• personal addresses</li> <li>• personal email addresses</li> <li>• social security number</li> <li>• date of birth</li> <li>• personal telephone numbers</li> <li>• emergency contact information</li> </ul>	HTTPS secure protocol



<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
		<ul style="list-style-type: none"> <li>• healthcare insurance beneficiary account numbers</li> <li>• current medications</li> <li>• prior medical authorization number and services</li> <li>• previous medical record</li> <li>• medical diagnosis codes</li> <li>• Medical diagnosis</li> <li>• Dates of treatment</li> <li>• physician name and contact information</li> <li>• Billed and Payable amounts</li> <li>• Physician Name,</li> <li>• Physician Tax Identification Number/SSN</li> <li>• Physician National Provider Identifier (NPI)</li> <li>• Certificate/License Number</li> <li>• Physician Telephone</li> <li>• Physician Address</li> <li>• Physician Email Address</li> </ul>	

**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:** Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

**Mitigation:**

- CLFM adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- Both contractor and VA employees, including those at VHA/CBO, are required to take Privacy, HIPAA, and information security training annually.
- All employees with access to Veteran’s information are required to complete the VA Privacy and

- Information Security Awareness training and Rules of Behavior annually
- Information is shared in accordance with VA Handbook 6500.

## 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*

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be</i>	<i>List the method of transmission and the measures in place to secure data</i>

			<i>more than one)</i>	
ClaimsNet	Claim Processing Information	Name Health Insurance plan beneficiary numbers Medical record Dates of health care service Medical procedures Financial Account Information TIN (SSN)	PWS	sFTP via VL Trader
Pharmacy PBN	Pharmacy reimbursement	Name Address DOB SSN	PWS	sFTP via VL Trader

**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:** PII or PHI could be compromised and used for nefarious purposes

**Mitigation:** VA employees and contractors follow procedures designed to mitigate risk of PII/PHI falling into the wrong hands. Annual training along with restrictive access processes greatly reduces the risk of information being compromised.

## 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.*

Yes, written notice is provided to each individual when they elect to receive care from the VA. System of Records Notice SORN is clear about the use of the information, specifically 13VA047 “Individuals Submitting Invoices-Vouchers For Payment-VA”; routine use is under revision and 23VA10NB3 “Non-VA Fee Basis Records-VA.( <https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E920911.pdf> )

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

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

Information disclosure is mandatory; benefits will not be paid unless subject’s information is obtained and used to process the medical claims. Camp Lejeune family members can decline to provide the requested information but if any or all the requested information is not provided, it may delay or result in denial of their request for Camp Lejeune Family Member Health Care Program (CLFMP) benefits.

**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*

Information disclosure is mandatory; benefits will not be paid unless subject's information is obtained and used to process the medical claims. Individuals are not directly asked to consent to this use of their information. However, they may choose to remove consent. Removal of consent may result in denial of claims or benefits.

If an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA Regional Office, a list of where can be found at:

<https://www.benefits.va.gov/benefits/offices.asp>

#### **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:** Veterans and members of the public may not know VA maintains, collects and store data

#### **Mitigation:**

- FSC mitigates this risk by clarifying CLFM's role through this PIA and the SORNs covering the systems which interact with CLFM. Individuals upon are request are referred back to the source system owner or sponsor, etc.
- Benefits will not be paid unless subject's information is obtained and used to process the medical claims.

## **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 may access their information via FOIA and Privacy Act procedures. In order to [vafscprivacyofficer@va.gov](mailto:vafscprivacyofficer@va.gov) submit an official FOIA or Privacy Act Request, individuals are provided the contact information for the FSC Privacy/FOIA Officer

## **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.*

Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. Appeals must be received within two years of the date of this EOB. If you disagree with the payment or decision regarding this medical claim, you need to send a copy of this EOB along with a written reason stating why you disagree with the payment or decision to the following Appeal address: DEPARTMENT OF VETERANS AFFAIRS, Financial Services Center, Camp Lejeune Family Member Program, PO Box 149200 Austin, TX 78714-9200

## **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.*

- Individuals are made aware of the procedures for correcting his/her information through the notice at collection.
- Procedures and contact information for correcting inaccurate or erroneous information is included on the EOB provided to the patient.

Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. Appeals must be received within two years of the date of this EOB. If you disagree with the payment or decision regarding this medical claim, you need to send a copy of this EOB along with a written reason stating why you disagree with the payment or decision to the following Appeal address: DEPARTMENT OF VETERANS AFFAIRS, Financial Services Center, Camp Lejeune Family Member Program, PO Box 149200 Austin, TX 78714-9200

#### **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 ensure data accuracy.*

- Veterans and family members have the ability to correct/update their information online via the VA's eBenefits website.
- <http://benefits.va.gov/benefits/offices.asp>

#### **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:**

Inaccurate data may be used to process claims.

**Mitigation:**

FSC verifies claim information data against medical authorizations; FSC relies on the data collected by VHA and has clear redress procedures in place. See the PIAs for Vista, CPRS, and eBenefits for the VA's mitigation efforts. Data is collected from VHA to accurately process medical claims in accordance with SORN 13VA047.

## **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.*

- Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation
- Once training and the security investigation are complete, a request is submitted for access. Before any access is granted, this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.



**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.*

- Contractors will have access to the system and their contracts are reviewed on an annual basis.
- Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed security investigation.
- Once training and the security investigation are complete, a request for access is submitted before any access is granted. This request must be approved by the government supervisor, Information Security Officer (ISO), and Office of Information & Technology (OIT).

**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.*

Talent Management System courses:

VA 10176: Privacy and Info Security Awareness and Rules of Behavior;

VA 10203: Privacy and HIPAA Training

VA 3812493: Annual Government Ethics

**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, 8 July 2021*
3. *The Authorization Status, Authorization to Operate ATO (HCPS)*
4. *The Authorization Date, 17 August 2021*
5. *The Authorization Termination Date, 27 August 2022*
6. *The Risk Review Completion Date, 5 August 2021*

7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH). High

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

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.*

No

### 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.*

N/A

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

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

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

N/A

**9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?*

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

N/A

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

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

N/A There is no RPA associated with CLFMP.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>

<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Princess Miller**

---

**Information System Security Officer, Rito-Anthony Brisbane**

---

**Information System Owner, Jonathan Lindow**

## 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).

- System of Records Notice SORN is clear about the use of the information, specifically 13VA047 “Individuals Submitting Invoices-Vouchers For Payment-VA”; routine use is under revision and 23VA10NB3 “Non-VA Fee Basis Records-VA.( <https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E920911.pdf> )

**Privacy Act Information:** The authority for collection of the requested information on this form is 38 USC 1787. The purpose of collecting this information is to determine your eligibility for reimbursement of health care related to conditions determined to result from contaminated water while you resided at Camp Lejeune, North Carolina, for a period of at least 30 days. The information you provide may be verified by computer matching programs with authoritative sources such as the Civilian Health and Medical Program of the Department of Veterans Affairs (CHAMPVA), Department of Defense (DoD), Defense Enrollment Eligibility Reporting System (DEERS), Centers for Medicare & Medicaid Services (CMS) or any other applicable authoritative source at any time. You are requested to provide your social security number as your VA record is filed and retrieved by this number. You do not have to provide the requested information on this form but if any or all of the requested information is not provided, given the form's purpose of establishing eligibility for the Camp Lejeune Family Member Program, it may delay or result in denial of your request for Camp Lejeune Family Member Program benefits. Failure to furnish the requested information will have no adverse impact on any other VA benefit to which you may be entitled. The responses you submit are considered private confidential and may be disclosed outside VA only if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records number 23VA16. For example, information including your social security number may be disclosed to the Department of Defense, contractors, trading partners, health care providers and other suppliers of health care services to determine your eligibility for medical benefits and payment for services.