



Privacy Impact Assessment for the VA IT System called:

**General Counsel Legal Automated Workload  
System (GCLAWS) Cloud  
VA Central Office  
Office of General Counsel**

**2255**

Date PIA submitted for review:

11/14/2023

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Gregory Draves	gregory.draves@va.gov	202-904-9280
Alternate Privacy Officer	Jeffrey E. Swanberg	Jeffrey.e.swanberg@va.gov	253-209-8858
Information System Security Officer (ISSO)	Keneath Coleman	Keneath Coleman	202-461-5122 / C 202-437-1860
Information System Owner	Randy Trexler	randy.trexler@va.gov	814-793-2486

## Abstract

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

The Office of General Counsel (OGC) General Counsel Legal Automation Workload System (GCLAWS) Cloud is a suite of software used by Department of Veterans Affairs (VA) OGC staff for support of the activities of the VA’s legal practice organization.

## 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?*  
General Counsel Legal Automated Workload System (GCLAWS) Cloud, Office of General Counsel

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 VA General Counsel Legal Case Automation Workload System (GCLAWS) Cloud is the system that supports the activities of VA’s legal practice organization with case management tracking, correspondence control, and statistical analysis. Cases are generated from matters brought to the Office of General Counsel (OGC) for consideration, review, response, analysis, and/or comment. This system of records contains case tracking for time and personnel, as well as case facts and pertinent documents uploaded with case comment activity. The case may include data privileged under the attorney-client relationship. The entire repository is used to provide statistical and other information in response to legitimate and reasonable requests.

C. *Who is the owner or control of the IT system or project?*  
The OGC GCLAWS Cloud is VA-owned and operated.

### 2. Information Collection and Sharing

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

GCLAWS Cloud stores legal case matter data for approximately 1 million individuals associated with case records as Veterans, Veterans’ representatives, claimants, judges, attorneys, debtor trustees, employees, tort feasons, fiduciaries, Veteran Service Organization (VSO) contacts, injured persons, insurees, property custodians, spouses, witnesses, and practitioners. GCLAWS Cloud stores accreditation data for approximately 20,500 people (attorneys, Veterans’ representatives, and Veteran Service Organization (VSO) contacts).

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

GCLAWS Cloud stores legal case matter data and accreditation data.

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

My eBenefits Web Portal (EBN) consumes GCLAWS Cloud Accreditation data via a staging database managed by Enterprise Web Operations (WebOps). Stakeholder Enterprise Portal (SEP) consumes GCLAWS Cloud Accreditation data via a staging database managed by WebOps. WebOps manages the staging database through which EBN and SEP consumes GCLAWS Cloud Accreditation data. The accreditation data being shared is public information and includes (Registration Number, Name of accredited individual or VSO, Date Originally Accredited, Date Recertification Due, Date Recertified, and Date Accreditation Cancelled).

GCLAWS Cloud also shares data internally in the Tort Audit Report, with the Office of Resource Management, Diversity and Inclusion (ORMDI)/Office of Resource Management (ORM) for the Annual No FEAR report, and as requested for OGC strategic Planning, ad hoc management reports, and ad hoc OGC Staffing analysis, staffing and budget calculations.

G. *Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

The GCLAWS Cloud system operates with one web site and one database server host.

### 3. *Legal Authority and SORN*

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

44VA026, General Counsel Legal Automation Workload System (GCLAWS)–  
VA:<https://www.govinfo.gov/content/pkg/FR-2007-09-19/pdf/E7-18464.pdf>

01VA022 - Accreditation Records – VA: <https://www.govinfo.gov/content/pkg/FR-2013-12-20/pdf/2013-30227.pdf>

U.S.C. Title 38 Veterans Benefits, Sections 501, Rules and Regulation; 311, General Counsel; 5901, Prohibition Against Acting as Claims Agent or Attorney; 5902, Recognition of Representatives of Organizations; 5903, Recognition With Respect to Particular Claims; and 5904 Recognition of Agents and Attorneys Generally.

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

The SORNs are being revised and will need approval once the revision is completed.

#### 4. System Changes

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

Completion of this PIA will not result in circumstances requiring changes to the business processes.

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

No

## 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 (II), 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. It must also match the information provided in question 3.4 of the PTA.*

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Name                     | <input type="checkbox"/> Emergency Contact                       |
| <input checked="" type="checkbox"/> Social Security Number   | Information (Name, Phone Number, etc. of a different individual) |
| <input checked="" type="checkbox"/> Date of Birth            | <input checked="" type="checkbox"/> Financial Information        |
| <input type="checkbox"/> Mother's Maiden Name                | <input checked="" type="checkbox"/> Health Insurance             |
| <input type="checkbox"/> Personal Mailing Address            | Beneficiary Numbers  |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | Account numbers  |
| <input checked="" type="checkbox"/> Personal Fax Number      |  |
| <input checked="" type="checkbox"/> Personal Email Address   |  |

Certificate/License numbers<sup>1</sup> (U.S. Jurisdiction, State, Territory Bar Membership or Registration Numbers; State or Federal Court Bar Membership or Registration Numbers)  
 Vehicle License Plate Number  
 Internet Protocol (IP) Address Numbers

Medications  
 Medical Records  
 Race/Ethnicity  
 Tax Identification Number  
 Medical Record Number  
 Gender  
 Integrated Control Number (ICN)

Military History/Service Connection  
 Next of Kin  
 Other Data Elements (list below)

Other PII/PHI data elements: No additional PII/PHI data elements are collected.

### PII Mapping of Components (Servers/Database)

**GCLAWS Cloud** consists of **seventeen** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **GCLAWS Cloud** 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.**

---

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Internal Components Table

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS (CPG)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (Confidential)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (02)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS (022)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (027)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (Docket)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS (023)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (024)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (025)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication



<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS (026)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (Common)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (Ethics)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS (National)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS (Research)	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS Cloud API	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
GCLAWS Cloud Web Client	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication
GCLAWS Cloud Outlook Client	Yes	Yes	Name, SSN, Home Address, DOB, Phone Number, e-mail, Financial Account Information, Health Insurance Beneficiary Numbers, Fax Number	Used to identify, contact, or locate a person (Veteran, claimant, appellant, etc.) related to a given legal case and in the processing of that case.	Access and permissions to the data is granted thru PIV/Windows Domain Authentication

## 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?*

Information is collected directly from the accredited representative, attorney or claims agent via VA Forms 21 and 21a as part of an accreditation request or as a part of authorized access to VA medical records. Information is collected directly from the Veteran via SF-95 for claims regarding Tort Claims. Data is also collected from clients via secure SharePoint portal.

*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.*

Information from other sources is not required.

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

The system does not create 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?*

Information is collected directly from the individual via documentation and forms they submit directly or via secure SharePoint portal.

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

Information for accredited representatives, attorneys, and claims agents is collected via OMB No. 2900-0018, VA Form 21, and OMB No. 2900-0605, VA Form 21a. Veteran information for tort claims is collected via OMB NO. 1105-0008, SF 95.

### **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.*

Checks for accuracy, completeness, and validity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system can check the accuracy, completeness, and validity of information inputs is guided by organizational policy and operational requirements.

*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?*

The system 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*

A System of Record Notification (SORN) GCLAWS (144VA026) was published in the Sept. 19, 2007, Federal Register. Pursuant to the Privacy Act, U.S. Code (U.S.C.) Title 5 Section 552a, OGC collects Veteran PII for Tort Legal Matters that are reportable medical malpractice and non-medical malpractice cases in which legal assistance has been rendered to VA clients where perfected administrative tort claims (specific allegation(s), sum certain, dated and signed by proper claimants) alleging injury or death, or property damage by reason of VA negligence, have been received. Authority for maintenance of the system is given under U.S.C. Title 38 Veterans Benefits, Sections 501, Rules and Regulation and 311, General Counsel. Authority to collect the information is provided in Code of Federal Regulations (C.F.R.) 28 Judicial Administration, Part 14 Administrative Claims Under Federal Tort Claims Act; U.S.C. Title 28 Judiciary and Judicial Procedure, Section 501 and the following, Section 2671 and the following; U.S.C 38 Veterans Benefits Sections 5902 Recognition of Representatives of Organizations and 5904 Recognition of Agents and Attorneys Generally; and C.F.R. 38 Pensions, Bonuses, and Veterans' Relief Part 14.629(b) Accreditation of Agents and Attorneys

### **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:** GCLAWS Cloud collects PII on Veterans and members of the public to support OGC's mission of providing legal advice and services to the SECVA and all organizational components of the Department by providing OGC with the means to track legal workload and deliver timely advice. The magnitude of harm if privacy or health-related data is disclosed is:

- Exposure of Veteran data can reveal embarrassing details of medical treatment/mishaps causing emotional distress.
- Exposure of data can subject individuals to an increased risk of harm from identify theft, fraud, or other injury.
- Exposure of data could result in individuals having to expend time and money to prevent future fraud, such as signing up for credit monitoring, contacting credit reporting agencies and placing fraud alerts on their accounts, etc.
- Exposure of data can result in an embarrassment to Secretary or other VA managers.

**Mitigation:** Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption (data at rest) and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors. The information stored in the system and accessed by VA OGC employees includes legal case matter workload data, regulations data, and accreditation data. For accreditation data, only information about accredited individuals that is already public is available to people external to the VA via the www.va.gov website. No individual outside of VA has access to the data stored within the system. The system is designed to allow only authorized users, OGC attorneys and support staff, access to subject matter databases on a need-to-know basis and can be made available to any OGC employee as necessary.

## **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 as an identifier	Used as an identifier
SSN	Used as an identifier	Used as an identifier
Home Address	Used as an identifier and if correspondence needs to be sent to the Veteran.	Used as an identifier and if correspondence needs to be sent to the Veteran.
DOB	Used as an identifier	Used as an identifier
Phone Number	Used to contact Veteran	Used to contact Veteran
E-mail address	Used to contact Veteran	Used to contact Veteran
Financial Account information	Used as an identifier	Used as an identifier
Health Care Beneficiary Numbers	Used as an identifier	Used as an identifier
Gender	Used as an identifier	Used as an identifier

## **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?*

Software is written in house and accessed by authorized users to analyze data using SQL queries, MS Excel, MS Power BI and MS Visual Studio.

*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.*

New data may be produced in the form of a text file or Excel document and any file that includes PII is handled in a secure way and if shared as required for business purposes it is done in a secure manner either via encrypted e-mail, secure fax or secure SharePoint site.

## **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?*

When the application runs within a user's web browser, all data is encrypted in transit using hypertext transfer protocol secure (HTTPS), which is the primary method to transfer data between a web browser and a web site. At the middle tier, the communications between web site and database is secured using Windows Authentication with the database source; this removes any username or password credentials stored within the connection configuration information. Connection configuration information is not embedded within the application code, rather it's stored in secured configuration files outside the application. Connection String information that is stored within the database are secured only to trusted users. Although there are several methods for securing the middle data access layer, Secure Socket Layer (SSL) encryption is not currently enabled at this level due to the impact on application performance; however, it can be enabled at any time. At the data storage level, all databases are encrypted using Transparent Data Encryption (TDE) at the file level when the data is at rest. McAfee Endpoint security is on the database servers to protect from network and file share threats.

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

At the application level, the web-based application masks all Social Security Numbers (SSNs) except the last four digits. Other protections in place include omitting SSNs from any reports.

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

GCLAWS Cloud uses VA's Governance, Risk and Compliance (GRC) tool, eMASS, to ensure all administrative, technical and physical safeguards are in place and reviewed in accordance with Government policy and standards. All OGC employees are required to complete VA Privacy and Information Security Awareness training and sign a Rules of Behavior annually as part of these safeguards.

## **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?*



OGC managers and their proxies request access for new users by submitting a help ticket via yourIT and the template they use for this request instructs them to be specific about the type of access (basic or administrative) the new user needs. Authorized users, OGC attorneys and support staff are granted access to subject matter databases on a need-to-know basis and as necessary for their job duties, as determined by GCLAWS Cloud documented standard operating procedures.

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

Yes, GCLAWS Cloud criteria, procedures, controls, and responsibilities regarding access are documented within Standard Operating Procedures.

*2.4c Does access require manager approval?*

Yes. Manager approval is implicit with the manager's or manager proxy's request for access.

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

Access is monitored for all users through access control logs and application logs.

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

All OGC employees and GCLAWS Cloud authorized users are responsible for safeguarding PII. Additionally, users are required to sign the Rules of Behavior annually. The ISO is responsible for assuring that all proper measures are taken to ensure confidentiality of PII on all systems for which they are responsible.

## 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
- SSN
- Home Address,
- DOB
- Phone Number,
- e-mail
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Gender

### 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.*

The “OGC Records Retentions Policy” identifies by Product Category the type of data that CAN be destroyed (or must be retained indefinitely) and the number of days the record must be retained by law. Some cases may be held longer than their retention period if they are included in a Litigation Hold. OGC does retain name, product category, case number and date destroyed in an audit table after all other data pertaining to a case is destroyed. This audit data is kept for the purposes of informing clients and managers that OGC may have had a case at one time, but it met its retention period and was destroyed.

Information is retained based on the type of data as listed in the Records Control Schedule N1–15–06–002. in items: 1, 3-4, 7-8, 10-15, 17-27 and 29-31. Information will be retained indefinitely if “AllowDestroy” is No in the table below.

Category Name	RetentionPeriodInYears	AllowDestroy
Accreditation of Representatives	10	No
Appropriations/Fiscal	10	No
Attorney Fees for Claimant Representation	10	No
Benefits (N.O.C.)	10	No
Commitment	10	No
Compensation & Pension	10	No
Eligibility	10	No
Fiduciaries and Guardianships	10	No
Health Care Matters (N.O.C.)	10	No
Hospital Administration	10	No
Inspector General/Criminal Investigation/Law Enf	10	No
Military Personnel and Employee Claims	6	No
Patient Safety	10	No
State Licensing Board	4	No
Title 38 Actions	6	No
38 U.S.C. 8127 & 8128 Legal Support	10	Yes
Administrative Issuances	10	Yes
Advisory Committees	10	Yes
Alternative Dispute Resolution	10	Yes
Bioethics	10	Yes
Breach Notification and Incident Response	10	Yes
Business Transactions (N.O.C.)	10	Yes
Canteen Service	10	Yes
Cemetery Matters	10	Yes
Clinical Research Agreements	10	Yes
Collections	3	Yes

<b>Category Name</b>	<b>RetentionPeriodInYears</b>	<b>AllowDestroy</b>
Copyright and Trademark	10	Yes
Credentialing of Healthcare Personnel	1	Yes
Cross-Organizational Collaboration	10	Yes
Data Security	10	Yes
Data Transfer Agreements	10	Yes
Debarment and Suspension	10	Yes
Defective Tort Claims	7	Yes
Department Organization/Reorganization (38 USC 510)	10	Yes
E-Discovery	10	Yes
Economy Act	10	Yes
Employment Law (N.O.C.)	6	Yes
Enhanced Use	10	Yes
Environmental	500	Yes
Equal Employment Opportunity	6	Yes
Ethics	6	Yes
Expand Sharing	10	Yes
Federal Labor Relations Authority	6	Yes
Freedom of Information Act Appeals	10	Yes
Gifts to VA	10	Yes
Grievance Arbitration	6	Yes
Immigration Law	6	Yes
Information Disclosure and Privacy	10	Yes
Information Technology Law	10	Yes
Insurance	10	Yes
Intellectual Property	50	Yes
Knowledge Sharing	10	Yes
LMR Bargaining Proposals	6	Yes
LMR Labor Agreements Review	6	Yes
Loan Guaranty Actions	10	Yes
Mentoring - Given	10	Yes
Mentoring - Received	10	Yes
Merit Systems Protection Board	6	Yes
National Practitioner Data Bank	4	Yes
Nonprofit Corporations	10	Yes
Office of Special Counsel	6	Yes
OGC Committee/Workgroup	10	Yes
OPM Arbitration Review	6	Yes
Other Labor Relations	6	Yes
Pay and Benefits	6	Yes
Personnel Action Review	6	Yes
Political Activities	6	Yes
Privacy Act Access Appeals	10	Yes
Privacy Act Amendment Appeals	10	Yes
Procurement-Construction	3	Yes
Procurement-Services	6	Yes
Procurement-Supply	6	Yes
Professional Education	10	Yes
Real Property-Easements	10	Yes
Real Property-Land Acquisition or Disposal	10	Yes

Category Name	RetentionPeriodInYears	AllowDestroy
Real Property-Leases	10	Yes
Reasonable Accommodation	3	Yes
Records and Information Management	10	Yes
Representation Requests	6	Yes
Research	10	Yes
Revocable Licenses	10	Yes
Section 504	10	Yes
Specialty Panel	10	Yes
Title IX	10	Yes
Title VI	10	Yes
Tort Claims - Medical Malpractice	7	Yes
Tort Claims - Personal Injury (Non Med Mal)	7	Yes
Tort Claims - Property Damage (Non Med Mal)	7	Yes
Touhy Regulations	10	Yes
Training - Given	10	Yes
Training - Received	10	Yes
Transitional Loan Housing Program	10	Yes
VBA Burial Benefits	10	Yes
Vocational Rehabilitation and Education	10	Yes
Employee Development	10	No
Security/Law Enforcement	10	Yes
Federal Records Act	10	Yes
Financial Mgmt.	10	Yes
Human Resource Mgmt.	10	Yes
Information Disclosure	10	Yes
Information Resource Mgmt	10	Yes
Management and Operations	10	Yes
Office Operations	10	Yes
Paperwork Reduction	10	Yes
Site Visit	10	Yes

### 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?*

Yes. Records Control Schedule N1-15-06-2, [res10-1.pdf \(va.gov\)](#), was approved by the Archivist of the United States on March 7, 2007 See 3.3b, below.

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

Records Control Schedule N1-15-06-2, [rcs10-1.pdf \(va.gov\)](#), was approved by the Archivist of the United States on March 7, 2007.

### **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.*

OGC managers or delegated personnel review lists of cases that have met retention period requirements and are ready for destruction. The reviewers can review records listed and either agree a record is ready for destruction or they can save a record from destruction, for example, if that record is part of a Litigation Hold. The electronic record is destroyed when a background job is run that deletes all data for that case except for the case name and type and the date of destruction, which are kept in an audit table for purposes of OGC knowing that a case may have existed at one time but was destroyed on given date. This process has been approved by the Information System Owner (ISO). Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)".

### **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.*

For testing and training, PII is either used as is or scrubbed. If used as is, individuals performing the testing or training and the audience are authorized to view the PII. PII is not used for research. Access to data is granted on a need-to-know basis and policies within the VA and OGC are followed for privacy training.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The*

*proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.*

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

*Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?*

*Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*

*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:

**Privacy Risk:** If data is retained beyond its record schedule and a breach occurs, then more data would be impacted.

**Mitigation:** OGC mitigates this risk by generating and reviewing the Expired Records Report based on the Records Retention Schedule. The review result is forwarded to the GCLAWS Cloud Operations and Sustainment Team for backend destruction.

## **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*

<b>List the Program Office or IT System information is shared/received with</b>	<b>List the purpose of the information being shared /received with the specified program office or IT system</b>	<b>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</b>	<b>Describe the method of transmittal</b>
Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), Board of Veteran Appeals (BVA)	Collaboration with other VA offices may be required to complete work product	Veteran Health and Claim - Information: SSN, Name, Date Of Birth, Address, Full Health Record	OGC SharePoint, Email, Phone, and Fax
VHA, VBA, NCA, Staff Offices	Collaboration with other VA offices may be required to complete work product	Personnel Records and Labor/Employee Relations: SSN, Name, Date Of Birth, Address	OGC SharePoint, Email, Phone, and Fax
Enterprise Veterans Self Service Portal (EVSS) Services Tier, formerly eBenefits Web Portal (EBN) (VASI #1093)	Provide individuals/Veterans seeking representation services before VA with information on individuals currently accredited by VA and organizations currently recognized by VA	Public Accreditation data	Staging database managed by VA Web Operations
Enterprise Veterans Self Service Portal (EVSS) Portal Tier, formerly Stakeholder Enterprise Portal) (SEP) VASI #1608)	Provide individuals/Veterans seeking representation services before VA with information on individuals currently accredited by VA and organizations currently recognized by VA	Public Accreditation data	Staging database managed by VA Web Operations

<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>
Enterprise Web Infrastructure (WebOps) (VASI #2645)	Provide individuals/Veterans seeking representation services before VA with information on individuals currently accredited by VA and organizations currently recognized by VA	Public Accreditation data	SQL Query connection
Corporate Data Warehouse (VASI #1152)	Collaboration with other VA offices may be required to complete work product	Base case information with no PII or PHI: Case ID, Case No, Category ID, Assigned To ID, Date Entered, Date Closed; Task Elements: Task Element ID, Task Type ID, Assigned To ID, Date Entered, Date Closed; Case Time/Note Case Task Element ID, Owned By ID, Date Of Event, Date Entered, Time Spent; User GUID, Name, Station ID, Active Status; Facility ID, Facility Name, Station ID, VISN City/State/Region	SQL Query connection
Tort Audit Report	Validation and summary of tort judgements	Record Number, Date Claim Filed, Date of Case Status, Case Status Code, Date Received, Date of Incident, Total Amount Claimed, Judgement Amount, Date Closed, Allowed Amount	Email
Office of Resource Management, Diversity and Inclusion (ORMDI)/Office of Resource Management (ORM)	Compliance with the reporting provisions of the No FEAR Act	Annual No FEAR Report: Discrimination Type, Discrimination Statute Type, EEO Decision Type, Dollar Amount Paid To Plaintiff, Attorney Fees, Basis Of Finding (totals only)	Email and VA Integrated Enterprise Workflow Solution (VIEWS)



<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>
Ad Hoc Freedom of Information Act (FOIA) Requests	Compliance with the FOIA	Varies per request	Per request (e.g., (Email, Fax, Paper, etc.))
Ad Hoc Management Reports	Varies per request	Varies per request	Per request (e.g., OGC SharePoint, PowerBI, Email, Phone, Fax, etc.)
OGC Strategic Planning	Strategic planning	Varies per request	Per request (e.g., OGC SharePoint, PowerBI, Email, Phone, Fax, etc.)
OGC Staffing Analysis / Ad Hoc Staffing/Budget Calculations	Staffing analysis and staffing and budget calculations	Varies per request	Per request (e.g., OGC SharePoint, PowerBI, Email, Phone, Fax, etc.)

#### **4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

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

Follow the format below:

**Privacy Risk:** There is a risk that PII could be shared unencrypted.

**Mitigation:** No one outside of OGC and authorized OIT staff has direct access to OGC GCLAWS Cloud data. Data may be shared with VA employees and contractors who have been vetted, gone through privacy and security training, and have signed nondisclosure agreements. Data is transmitted via secure/encrypted e-mail, OGC SharePoint site where only OGC employee have access, phone, or secure fax.

## 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

<b>List External Program Office or IT System information is shared/received with</b>	<b>List the purpose of information being shared / received / transmitted with the specified program office or IT system</b>	<b>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</b>	<b>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</b>	<b>List the method of transmission and the measures in place to secure data</b>
External Financial Auditors	Providing data for annual audits.	Veteran Claim Information (SSN, Name, Date Of Birth, Address)	GCLAWS SORN-(144VA026 ) routine use as outlined in the Federal Register published 9/19/07	OGC SharePoint, Email, Phone, and Fax
Health Insurance Companies	Collaboration with health insurance companies required for Medical Care Cost Recovery (MCCR).	Veteran Health and Billing Information (SSN, Name, Date Of Birth, Address, Full Health Record)	GCLAWS SORN-(144VA026) routine use as outlined in the Federal Register published 9/19/07	OGC SharePoint, Email, Phone, and Fax
Bank Entities	Collaboration with banks required for case matters dealing with mortgages.	Veteran Claim Information (SSN, Name, Date Of Birth, Address)	GCLAWS SORN-(144VA026) routine use as outlined in the Federal Register published 9/19/07	OGC SharePoint, Email, Phone, and Fax

<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 more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
Structured Settlement Companies	Collaboration with banks required for case matters dealing with structured settlements.	Veteran Health Information (SSN, Name, Date Of Birth, Address, Partial Health Record)	GCLAWS SORN-(144VA026) routine use as outlined in the Federal Register published 9/19/07	OGC SharePoint, Email, Phone, and Fax
Department of Justice	Providing data annual reports that go to Dept. of Justice	Veteran Health and Claim Information (SSN, Name, Date Of Birth, Address, Partial Health Record)	GCLAWS SORN-(144VA026) routine use as outlined in the Federal published 9/19/07	OGC SharePoint, Email, Phone, and Fax
Employment Law Third-Party Adjudicators and Investigators	Providing information for Litigation and Settlement	Veteran Health and Claim Information (Name, Date Of Birth, Address, Partial Health Record)	GCLAWS SORN-(144VA026) routine use as outlined in the Federal published 9/19/07	OGC SharePoint, Email, Phone, and Fax, Third-Party Secure Websites

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a*

*Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** There is a risk that data could be shared unencrypted.

**Mitigation:** No one outside of OGC and authorized OIT staff has direct access to OGC GCLAWS Cloud data. Data may be shared with VA employees and contractors who have been vetted, gone through privacy and security training, and have signed nondisclosure agreements. Data is transmitted via secure/encrypted e-mail, OGC SharePoint site where only OGC employees have access, phone, or secure fax.

## 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.*

OGC GCLAWS SORN (144VA026) was published in the Federal Register in 2007 (72 Fed. Reg. 53662 (Sept. 10, 2007)) (<https://www.govinfo.gov/content/pkg/FR-2007-09-19/pdf/E7-18464.pdf>). Accreditation Record –VA SORN (01VA022, amended) (<https://www.govinfo.gov/content/pkg/FR-2013-12-20/pdf/2013-30227.pdf>) was published in the Federal Register in 2013 (78 Fed. Reg. 77206).

Standard Form (SF) 95 Claim for Damage, Injury, or Death used to submit Tort Claims (<https://www.gsa.gov/system/files/SF95-07a.pdf>), VA Form 21 Application for Accreditation as Service Organization Representative (<https://www.va.gov/vaforms/va/pdf/VA21.pdf>), and VA Form 21a Application for Accreditation as a Claims Agent Or Attorney (<https://www.va.gov/vaforms/va/pdf/VA21a.pdf>) each have a Privacy Act Notice.

Version date: October 1, 2023

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

See Appendix A-6.1 for copies of the Privacy Act Notices on SF 95, VA Form 21, and VA Form 21a.

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.

Those affected or their agents initiate the collection of their information by voluntarily completing SF 95 and VA Forms 21 and 21a. The Privacy Statements on those forms clearly state the purpose for the collection of the information and its routine uses.

**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.*

Providing PII is required to gain access to systems associated with performing job duties, as well as a condition of employment. For Tort Claims, the back of the SF-95 annotates that disclosure is voluntary, but failure to completely fill out the form or provide requested materials may render the claim invalid. For Accreditations, VA Forms 21 and 21a clearly state providing the information is voluntary but failure to provide full information could delay or preclude accreditation or delay or prevent action on the application.

**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 consent to use of their information in all the uses identified on SF 95 and on VA Forms 21 and VA21a when they or their agents submit that information.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

*Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** If sufficient notice is not provided, then there is a risk that individuals' reluctance to provide required information will lead to adversely affecting their claim or application.

**Mitigation:** For Tort Claims, the privacy notice was published in the Sept. 19, 2007, Federal Register and is provided on the back of the SF-95. For Accreditations, the privacy notice was published in the Dec. 20, 2013, in the Federal Register and on VA Forms 21 and 21a. The privacy notices on the forms clearly state the consequences of not supplying requested information.

## 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.*

Individuals may request information GCLAWS Cloud may have on them either via a Freedom of Information Act (FOIA) (via the VA Freedom of Information Act Public Access Website, <https://vapal.efoia-host.com/app/Home.aspx>) or a Privacy Act Request. Individuals who wish to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request to the Deputy General Counsel, Office of General Counsel, U.S. Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. Requests for correction of information reported by the Office of the General Counsel's online accreditation search application may be sent to the Accreditation Mailbox [ogcaccrreditationmailbox@va.gov](mailto:ogcaccrreditationmailbox@va.gov).

*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)?*

GCLAWS Cloud was designed for use by the Office of General Counsel to facilitate the delivery of legal services to the Department. The records entered into GCLAWS are entered there in anticipation of litigation. Therefore, the records in GCLAWS Cloud are exempt from the access and amendment requirements of the Privacy Act.

Per 5 U.S.C. § 552a(d)(5) Special Exemption for Information Compiled for Civil Action: “[N]othing in this [Act] shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.” Per the Department of Justice (DOJ) (The “Overview of the Privacy Act of 1974,” prepared by the DOJ Office of Privacy and Civil Liberties (OPCL)), Information compiled in anticipation of civil litigation is exempt from the Privacy Act’s access and amendment provisions:

The subsection (d)(5) provision is sometimes overlooked because it is not located with the other exemptions in sections (j) and (k). On its face, it is only an exemption from the access provisions of the Privacy Act, but by implication, it also operates as an exemption from the amendment provisions. See, e.g., *Smith v. United States*, 142 F. App’x 209, 210 (5th Cir. 2005) (per curiam) (holding that plaintiff had no right to amend record that was “prepared in response to [his] [Federal Tort Claims Act] claim” because it fell within coverage of the exemption to access in subsection (d)(5) and, therefore, was “also exempt from the amendment requirements of the Act” (emphasis added)).

*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?*

GCLAWS Cloud is a Privacy Act System of Records.

## **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.*

Requests for data correction can be made through the Deputy General Counsel, Office of General Counsel, U.S. Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420.

## **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.*

Information contained in GCLAWS Cloud is exempt from the access and amendment provisions of the Privacy Act pursuant to 5 U.S.C. § 552a(d)(5).

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



*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.***

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

Redress is provided as listed above. Individuals can contact OGC for formal redress.

## **7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction**

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

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

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

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

*Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*

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

Follow the format below:

**Privacy Risk:** If individuals do not have access to their information stored in OGC databases then incorrect data can exist and may go uncorrected.

**Mitigation:** Individuals may contact OGC to see what, if any, data regarding them is stored along with procedures to notify OGC if any data correction is needed.

## **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?*

Procedures for setting up users with access are documented via Standard Operating Procedures (SOPs). The steps managers must follow also are within the new employee notices OGC Human Resources sends to managers. Managers are instructed to input a yourIT ticket and provide the date the user signed the Rules of Behavior. Managers are also instructed to specify exactly what type of access the new employee requires.

*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Users from other agencies do not have access to the system.

*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.*

The system is designed to allow only authorized users, OGC attorneys and support staff, access to subject matter databases on a need-to-know basis and can be made available to any OGC employee as necessary. Database roles are assigned to users where the basic role allows users to enter in case and time information for themselves, management roles allow access to view time entries for all users and the case maintenance role allows access to case maintenance forms for review of expired cases.

**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 may have access to sensitive information in the production or nondevelopment environment to sustain the system with enhancements and break/fix changes, and to keep the system compliant. Contractors must acknowledge awareness of security practices via annual VA Privacy Security Awareness (PISA) and Rules of Behavior training certifications.

**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.*

OGC Talent Management System (TMS) administrators and the ISO use the VA TMS for tracking all training records. All OGC users are required to take Information Security Awareness, Health Insurance Portability And Accountability Act (HIPAA) and Privacy Act Training and those records are maintained by employees, supervisors, and management. Management reviews the status of training requirements and track progress. The VA Office of Human Resources is responsible for maintaining security and privacy awareness training records for each employee. Also, the system-use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen of each application until the user takes explicit actions to log on to the information system. OGC also provides training, not captured in TMS, to its staff regarding the sensitivity of the records contained in GCLAWS.

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

*No.*

*8.4a If Yes, provide:*

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

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

*8.4b If No or In Process, provide your **Initial Operating Capability (IOC) date.***

The A&A is in progress with an IOC date estimated at 10/1/2024. The system was recently categorized as Moderate.

## **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)**

GCLAWS Cloud uses the Infrastructure as a Service (IaaS) model within the VEAC.

**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.**

<<ADD ANSWER HERE>>

**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.*

<<ADD ANSWER HERE>>

**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.*

<<ADD ANSWER HERE>>

**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).*

<<ADD ANSWER HERE>>

## 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>
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.**

---

**Privacy Officer, Gregory Draves**

---

**Information Systems Security Officer, Keneath Coleman**

---

**Information Systems Owner, Randy Trexler**


## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

The Privacy Notice on Standard Form (SF) 95 Claim for Damage, Injury, or Death (<https://www.gsa.gov/system/files/SF95-07a.pdf>) is shown below.

PRIVACY ACT NOTICE	
This Notice is provided in accordance with the Privacy Act, 5 U.S.C. 552a(e)(3), and concerns the information requested in the letter to which this Notice is attached. A. <i>Authority:</i> The requested information is solicited pursuant to one or more of the following: 5 U.S.C. 301, 28 U.S.C. 501 et seq., 28 U.S.C. 2671 et seq., 28 C.F.R. Part 14.	B. <i>Principal Purpose:</i> The information requested is to be used in evaluating claims. C. <i>Routine Use:</i> See the Notices of Systems of Records for the agency to whom you are submitting this form for this information. D. <i>Effect of Failure to Respond:</i> Disclosure is voluntary. However, failure to supply the requested information or to execute the form may render your claim "invalid."
PAPERWORK REDUCTION ACT NOTICE	
This notice is <u>solely</u> for the purpose of the Paperwork Reduction Act, 44 U.S.C. 3501. Public reporting burden for this collection of information is estimated to average 6 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Director, Torts Branch, Attention: Paperwork Reduction Staff, Civil Division, U.S. Department of Justice, Washington, DC 20530 or to the Office of Management and Budget. Do not mail completed form(s) to these addresses.	
<b>STANDARD FORM 95 REV. (2/2007) BACK</b>	

The Privacy Notice on VA Form 21 Application for Accreditation as Service Organization Representative (<https://www.va.gov/vaforms/va/pdf/VA21.pdf>) is shown below.

APPLICATION FOR ACCREDITATION AS SERVICE ORGANIZATION REPRESENTATIVE	
 U.S. Department of Veterans Affairs	Form Approved: OMB No. 2900-0018 Exp. Date: Feb 28, 2023 Respondent Burden: 15 minutes
<b>PRIVACY ACT AND PAPERWORK REDUCTION ACT NOTICE:</b> The information requested on this form is solicited under 38 U.S.C., Section 5902, which authorizes VA to recognize representatives of approved organizations for the preparation, presentation, and prosecution of claims under laws administered by VA. The requested information will enable VA to determine your eligibility for accreditation as a representative of a recognized service organization. Your disclosure of this information to us is voluntary, but your failure to provide full information could delay or preclude your accreditation. The Privacy Act authorizes VA to disclose the information outside VA for certain routine uses, which have been published in the Federal Register with reference to a VA system of records entitled, "Accreditation Records-VA" (01VA022). Such routine uses include verification of the identity, status, and service organization affiliation of representatives, civil or criminal law enforcement, communications with members of Congress of their representatives, Government litigation, and notification to service organizations of information relevant to a refusal to grant or a suspension or termination of accreditation.	
<b>RESPONDENT BURDEN:</b> VA may not conduct or sponsor, and you are not required to respond to, this collection of information unless it displays a valid OMB Control Number. The public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to VA Clearance Officer (005G2), 810 Vermont Avenue, NW, Washington, DC 20420. <b>Send comments only. Do not send</b> this form or requests for benefits to this address.	

The Privacy Notice on VA Form 21a Application for Accreditation as a Claims Agent Or Attorney (<https://www.va.gov/vaforms/va/pdf/VA21a.pdf>) is shown below.

**PRIVACY ACT INFORMATION:** The information requested on this form is solicited under Section 5904, Title 38, United States Code and Section 14.629(b) of Title 38, Code of Federal Regulations. It will enable VA to determine initial eligibility for accreditation as a claims agent or attorney to represent claimants before VA. Any information on this form may be disclosed outside VA only if authorized under the Privacy Act, including the routine uses identified in the VA system of records, 01VA022, Accreditation Records--VA, published in the Federal Register. Routine disclosures may be made for the following purposes: civil or criminal law enforcement or investigation; congressional communications; communications relevant to the delivery of VA benefits; verification of identity and status; litigation conducted by the Department of Justice; and communication with employing entities and governmental licensing organizations concerning information relevant to employment or licensing of a prospective, present, or former representative, claims agent or attorney. Providing the requested information is voluntary; however, failure to furnish information may delay or prevent action on the application.

**RESPONDENT BURDEN:** VA may not conduct or sponsor, and respondent is not required to respond to this collection of information unless it displays a valid OMB Control Number. Public reporting burden for this collection of information is estimated to average 45 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments regarding this burden estimate or any other aspect of this collection of information send your comments to VA Clearance Officer (005R1B), 810 Vermont Avenue, NW, Washington, D.C. 20420. Please do not send applications for accreditation to this address.

VA FORM 21a, APR 2020, PAGE 4

PREVIOUS VERSIONS OF THIS FORM WILL NOT BE USED.

### System of Records Notices:

- OGC GCLAWS SORN (144VA026) (<https://www.govinfo.gov/content/pkg/FR-2007-09-19/pdf/E7-18464.pdf>).
- Accreditation Record –VA SORN (01VA022, amended) (<https://www.govinfo.gov/content/pkg/FR-2013-12-20/pdf/2013-30227.pdf>).



## **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](#)