



Privacy Impact Assessment for the VA IT System called:

# Casepoint Government -E (CG-E)

## Enterprise Program Management Office

### Department of Veteran's Affairs, Corporate

Date PIA submitted for review:

December 29, 2021

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Scott Miller	Scott.miller@va.gov	215-600-9491
Information System Owner	Michael Vella	Michael.vella1@va.gov	973-836-9520

Version Date: October 1, 2021

Page 1 of 34

## Abstract

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

The Federal Rules of Civil Procedure (FRCP) require the VA to use an e-Discovery tool in order to effectively preserve, collect, process, review, analyze, and produce Electronically Stored Information (ESI). Casepoint Government -E (CG-E) is a Software as a Service (SaaS) product which immediately allows VA to preserve and produce ESI from VA email traffic, while maintaining obligations under FOIA, the Privacy Act of 1974, HIPAA, and other related legislation. CG-E searches existing VA email based on parameters defined by specific cases (persons, medical conditions, SSNs, military units, etc); holds those emails for further analysis; and places a legal hold on ESI found to have bearing on the specific case. FRCP requires VA to produce relevant ESI on “any non-privileged matter that is relevant to any party’s claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter,” Fed. R. Civ. P. 26(b)(1), regardless of the media, originality, and including data on personal devices or otherwise not defined as a Federal Record; failure subjects the VA to serious legal sanctions.

## 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?*

CG-E will be used for litigation support. It is owned by VA OI&T, Department of Veteran's Affairs staff located at the VA Austin Automation Center (AITC). The purpose of the platform is to assist in the preservation, processing (such as decryption and de-duplication), search, review, analysis, and production of Electronically Stored Information (ESI) during litigation. The tool will assist attorneys in accomplishing the required tasks more efficiently and effectively. Should VA's e-discovery methods be challenged, using dedicated hardware and software to accomplish tasks is likely to be legally defensible whereas tasks performed manually are not.

CG-E is a SaaS product which immediately allows VA to preserve and produce ESI from VA email traffic, while maintaining obligations under FOIA, the Privacy Act of 1974, HIPAA, and other related legislation. CG-E searches existing VA email based on parameters defined by specific cases (persons, medical conditions, SSNs, military units, etc); holds those emails for further analysis; and places a legal hold on ESI found to have bearing on the specific case. FRCP requires VA to produce relevant ESI on "any non-privileged matter that is relevant to any party's claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter," Fed. R. Civ. P. 26(b)(1), regardless of the media, originality, and including data on personal devices or otherwise not defined as a Federal Record; failure subjects the VA to serious legal sanctions.

The number of individuals with information in the system will be determined on case-by-case basis. Any relevant information involving pending or reasonably anticipated litigation stored in VA IT systems can become a part of the data stored in this system. Information in the VA IT systems may be in any form of digital media such as email, word processing, spreadsheets, databases, audio and images and may contain all forms of PII/PHI. It may be collected from VA exchange servers, file shares, voice mail, tablets, phones or any storage devices hosting digital data now or in the future. The system will produce reports generated by OGC staff as needed to support litigation.

The system is stand-alone and will not share information with other IT systems; however, the system will contain information that is collected from other IT systems. Additionally, as described in Section 5.1, information collected, processed, reviewed and produced may be shared with the Department of Justice (DOJ) and any parties to a lawsuit, who, under federal law, have a right to the information.

As described in section 1.4, the Federal Rules of Civil Procedure and other federal laws require the preservation and production of ESI. If VA fails to maintain ESI in pending or reasonably anticipated litigation it may be liable for spoliation of evidence and face court-imposed penalties, including a judgment and monetary damages against the VA. SORN 16VA026 states: 42 U.S.C. 2651 et seq.; 31 U.S.C. 3911; 28 U.S.C. 1346; 29 CFR 1600–1699; 38 U.S.C. 311 are the authorities to maintain the system.

The completion of this PIA will not result in a change of business operations/processes, technology changes or amendment to the SORN.

CG-E will be using the vendor's chosen cloud.

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

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

Information in the CG-E platform may be in any form of digital media such as email, word processing, spreadsheets, databases, audio and images and may contain all forms of SPI/III/IIHI/PHI. It may be collected from VA exchange servers, file shares, voice mail, tablets, phones, or any storage devices hosting digital data now or in the future. The system will produce reports generated by Office of General Counsel (OGC) staff as needed to support litigation. Information on any individuals involved in cases under investigation by OGC can become a part of the data stored in this system.

The system will not automatically collect any of the above information. In most cases, email is collected and would not contain most of the above types of data, however, since a lawsuit can involve any allegation related to any of VA’s employees, veterans or its mission, duties and programs, it is possible that any type of ESI that VA maintains could be collected and stored in CG-E.

**PII Mapping of Components**

<Information System Name> consists of <number> key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <Information System Name> and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

**Casepoint Government -E (CG-E)** consists of 02 key components (databases & File Share). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Casepoint Government -E (CG-E)** 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 the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

*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
Casepoint Government -E (CG-E)	Yes	Yes	CG-E receives emails from Outlook.	Any VA email traffic can be	Casepoint encrypts data at rest and

		<p>The potential for PII / PHI depends on the email traffic being reviewed;</p> <p>Name  Social Security Number  Date of Birth  Mother’s Maiden Name  Mailing Address  Zip Code  Phone Number(s)  Fax Number  Email Address  Emergency Contact Information (Name, Phone Number, etc. of a different individual)  Financial Account Information  Health Insurance Beneficiary Numbers  Account numbers  Certificate/License numbers  Vehicle License Plate Number  Internet Protocol (IP) Address Numbers  Current Medications  Previous Medical Records  Race/Ethnicity</p> <p>It is possible that any type of PII/PHI/SPI in the form of Electronically</p>	<p>reviewed and retained in CG-E, but is only provided to Courts as evidence (and is not otherwise shared). The information can be shared with Department of Justice and Federal, State, Local and Tribal Judicial courts/tribunals. It may be shared with legal counseling representing the person/entity in litigation with the VA.</p>	<p>Data in transit (AES 256-bit encryption)  The application uses minimum TLS 1.2 with an SSL certificate for protecting the confidentiality and integrity of transmitted data from the customer to the Casepoint Government - E (CG-E) authorization boundary. Casepoint enforces user of MFA and the application access is restricted to only certain Whitelisted IPs.</p>
--	--	--	---	--

			<p><b>Stored Information (ESI) that VA maintains (on any platform) could be collected and stored in CG-E and shared internally with OGC.)</b></p>	
--	--	--	---	--

**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.*

A case originates when VA knows or should know that information in any VA record or IT system is relevant to pending or reasonably anticipated litigation. At that time, a duty arises pursuant to federal law to preserve all VA ESI that is relevant to the litigation or that may lead to the production of relevant information. The system is designed so that VA personnel may electronically collect ESI from “custodians” (the VA employees that have the relevant information) and transfer it to CG-E for processing, review and production in litigation. Information in the CG-E platform may be in any form of digital media such as email, word processing, spreadsheets, databases, audio and images and may contain all forms of SPI/III/IIHI/PHI. It may be collected from VA exchange servers, file shares, voice mail, tablets, phones or any storage devices hosting digital data now or in the future, and all platforms capable of storing electronic data from all pillars of the VA. The data pulled from the VA IT system and imported into the CG-E system will be searched by OGC employees for information relevant to pending or reasonably anticipated litigation. Reports may be generated by OGC staff as needed to support litigation.

**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.*

Information will be collected by local VA Office of Information & Technology (OIT) staff pulling it from the native VA IT systems and delivered electronically to Department of Veteran's Affairs to be imported into CG-E. For example, a custodian's email account would be copied from the Exchange server by local OIT, and then sent encrypted to EMPO to be imported into CG-E.

All data is retrieved directly from VA devices to support litigation evidence. Individuals do receive notice or provide consent about data collected for litigation purposes.

#### **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.*

The CG-E system does not communicate with any outside systems to check data for accuracy. The purpose of the CG-E system is to collect ESI in the state that it is maintained. This is because the parties involved in litigation must be able to review the ESI in the form that it existed at the time the duty to preserve arisen. Wrongful alteration of evidence, including ESI, is improper under the rules of law.

#### **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*



As stated above, the preservation, collection and production of ESI is required by:

- The FRCP, which explicitly require parties in litigation to preserve and produce ESI;
- The Constitution, which empowers Congress to obtain information from federal agencies;
- The Freedom of Information Act (FOIA), which requires agencies to disclose information in electronic form; and
- The Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, both of which require that an individual be provided access to his/her own records, including electronic information.

Additionally, this system currently has full Authority to Operate. This PIA is completed to address system name change and request for a new ATO based on major system upgrade.

SORN 16VA026 states: 42 U.S.C. 2651 et seq.; 31 U.S.C. 3911; 28 U.S.C. 1346; 29 CFR 1600–1699; 38 U.S.C. 311 are the authorities to maintain the system.

### **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:** As a cabinet-level agency of the U.S. Government, the VA is required by law to preserve ESI, as stated previously. Moreover, in litigation, the VA is required to search all possible locations where evidence may be found. The privacy risk is mitigated by the attorneys working directly with relevant custodians to assess what information may be in the VA's possession, and then collecting that information.

**Mitigation:** Information is collected directly from VA IT systems and transferred to the CG-E platform electronically. Redaction of some information is required by law and further protects the privacy interests of any SPI that may appear in the data.

The information is then securely transferred to the CG-E system. The information may not be shared with anyone who is not a party to the litigation. Additionally, federal statutes require the redaction of certain information so that even when information is produced, it is redacted when required by law. Other federal laws allow for the withholding of information subject to privileges, such as the attorney-client privilege and attorney work product rule. Federal Rule of Evidence 501 describes the law of privilege in general.

## 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.*

OGC is responsible for representing the VA in all legal matters. To accomplish this purpose, VA must collect ESI relevant to any pending or reasonably anticipated litigation. ESI stored in VA IT systems is collected by the OIT, it is processed through CG-E and then it is reviewed for relevancy by OGC attorneys or staff. If a lawsuit has been filed, then the ESI will be shared with DOJ attorneys (see Section 5). ESI is then produced to opposing parties in litigation as required under the FRCP. Thus, ESI collected and stored in CG-E may be disclosed to parties in litigation; however, ESI stored in CG-E may only be produced to a party with a claim relevant to that ESI. For example, if Party A files an EEO claim against VA, then OGC may collect ESI relevant to Party A's claim, and VA may be required to produce relevant, unprivileged ESI to Party A and her attorney. However, nobody else will be given that information unless a judge orders its release. Moreover, as stated above, information is redacted before it is released when required by law. The data is non standardized and is collected from multiple E sources. Any portion of this data may contain information that could be used as evidence for litigation.

### **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*

CG-E sifts through large amounts of collected ESI to find documents, usually emails, MS Office or similar files. Those documents can then be searched for keywords or information relevant to litigation, which can be marked for future reference, collected into groups, etc. The system includes functionality for masking or redacting data as required by law. Once the information is organized and searched, it is reviewed by an attorney for relevance to the litigation and then may be redacted (if required by law) and produced to other parties in the litigation pursuant to the FRCP.

## **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?*

SC-9 & SC-28: Casepoint encrypts data at rest and data in transit using AES 256-bit encryption through Self-Encrypting Drives. The application uses TLS 1.2 with an SSL certificate for protecting the confidentiality and integrity of transmitted data from the customer to the Casepoint authorization boundary. Microsoft Azure encrypts all data rest on all the VMs, once Casepoint enables encryption on it. All servers and attached storage drives are encrypted using Azure Storage Service Encryption (SSE) which uses Azure Key Vault to create the encryption keys, and to use them for disk encryption and to store the keys. Azure Key Vault is used to encrypt keys that are stored in a FIPS validated hardware security module (HSM). When keys are imported or generated, Microsoft processes the keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware). With Key Vault, Microsoft doesn't see or extract the keys. Key use is monitored and audited by piping logs into SIEM for analysis and threat detection. All aspects of key management and usage are logged and monitored using SIEM. These logs flow into SIEM for auditing by the Casepoint Security Operations team.

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

Casepoint has multiple layers of security such as: IP whitelisting, Web Application Firewall, NSG (Network Security Groups), IDS/IPS, Access Control management via MFA and monthly access reviews, SIEM solution with 24 X 7 monitoring, and to add to the above: The Casepoint has configured the Casepoint Government -E (CG-E) application to use cryptographic mechanisms to prevent unauthorized disclosure and modification of customer data which is located on the disks attached to the server VMs and the SQL databases. See SC-28 for VM disk and database encryption

*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*

Casepoint implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission using logical security safeguards for ingress and egress boundary traffic, as well as traffic internal to its authorization boundary. (For more details please refer the SSP Section SC-8 Transmission confidentiality and Integrity & SC-28 Protection of Information at Rest, here SC-9 is redirecting to SC- 8 <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=SC-9>).

**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:

All attorneys have a legal obligation as officers of the court licensed to practice law in one of the fifty states to preserve the confidentiality of ESI. Attorneys may be subject to discipline by their state bar association and may lose their license to practice law if they improperly disclose information learned in the course of practicing law. Additionally, attorneys have an obligation to supervise staff working under their control to verify that staff is following the same confidentiality standards that attorneys must follow.

Use limitation is also controlled by the litigation. No party may access ESI stored in the CG-E system unless they have a right under the FRCP and other federal privacy laws. Also, CG-E has administrator-controlled permissions that can be set for each user to control what type of access they have to the system. See section 8.1.

## **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*

All information that is collected is not retained on the CG-E servers. Through a process called “pre-processing” and “processing,” systems files and other irrelevant files are deleted from the case file to prevent unnecessary use of server storage space and inadvertent disclosure of sensitive data not relevant to the case. The information that is retained is the emails, MS Office files and other relevant ESI including, but not limited to audio files, video files, image files, and PDFs.

### **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.*

All information that is collected becomes a part of the Office of General Counsel’s litigation case records. OGC’s official system of records for litigation cases is 16VA026. The retention period will vary on a case-by-case basis. The retention periods are explained further in the OGC Records Control Schedule. For example, Equal Employment Opportunity (EEO) cases must be preserved for four years after resolution of the case.

### **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.*

The VA Office of General Counsel Records Control Schedule (N1-15-06-2) has been approved by NARA. ESI in the CG-E system will become a part of official litigation case file, as described in section 3.2.

CG-E temporarily retains data for litigation cases involving the VA. Once the case is closed, ESI in the CG-E system will become part of the official litigation case file record. The data will be moved to ITOPS to be archived and will be retained in accordance with OGC records control schedule (RCS). It will also be retained in accordance with the OGC Records Control Schedule 10-1 March 2017: [http://center.spokane.med.va.gov/HIM/Records%20Management/VHA%20Records%20Control%20Schedule%20\(RCS\)%2010-1%20-%202017-03.pdf](http://center.spokane.med.va.gov/HIM/Records%20Management/VHA%20Records%20Control%20Schedule%20(RCS)%2010-1%20-%202017-03.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*

Disposition of Printed Data:

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

### **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*

Yes. The CG-E application is designed to be deployed behind the Firewall and other network security devices and is not “Web” facing. CG-E utilizes password protection for local accounts and user roles limiting case access to only those accounts with express permissions. In addition, CG-E in conjunction with Windows Local and Active Directory security to limit access to system files and case information.

The data used in test and development is standard data used in CG-E industry. The data does not contain any real PII.

### **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:** As described herein, information is pulled from VA IT systems into CG-E in response to legal requirements. Information may not be deleted until the legal need for the collection and preservation of ESI has passed. Cost to use the system increases as the amount of data collected increases. Additionally, the personnel and time required to review data in CG-E increases as the amount of data increases.

**Mitigation:** OGC does not collect more than the minimum information necessary to support litigation.

As previously described, information is purged from the system after the archive period has ended.

## **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><i>List the Program Office or IT System information is shared/received with</i></b>	<b><i>List the purpose of the information being shared /received with the specified program office or IT system</i></b>	<b><i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i></b>	<b><i>Describe the method of transmittal</i></b>
VA IT Operations and Services (ITOPS): 1.Outlook VA exchange servers 2.MS Office and MS Enterprise Servers	When OGC collects and processes data, the information is used to defend or prosecute lawsuits filed against or by the United States. In such cases, the information is used by the attorneys (VA and DOJ) who are assigned to the case. The attorney may discuss emails or MS Office files, for example, with the VA employees or other persons who are involved in the litigation. That is done through interviews and depositions with the persons who are relevant to the litigation.	Information in the CG-E platform may be in any form of digital media such as email, word processing, spreadsheets, databases, audio and images and may contain all forms of SPI/III/IIHI/PHI. It may be collected from VA exchange servers, file shares, voice mail, tablets, phones or any storage devices hosting digital data now or in the future, and all platforms capable of storing electronic data from all pillars of the VA.	Manual copy of data from VA Field Operations servers to VA CG-E servers



<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>
VA Office of General Counsel (OGC)	When OGC collects and processes data, the information is used to defend or prosecute lawsuits filed against or by the United States. In such cases, the information is used by the attorneys (VA and DOJ) who are assigned to the case. The attorney may discuss emails or MS Office files, for example, with the VA employees or other persons who are involved in the litigation. That is done through interviews and depositions with the persons who are relevant to the litigation.	Information in the CG-E platform may be in any form of digital media such as email, word processing, spreadsheets, databases, audio and images and may contain all forms of SPI/III/IIHI/PHI. It may be collected from VA exchange servers, file shares, voice mail, tablets, phones or any storage devices hosting digital data now or in the future, and all platforms capable of storing electronic data from all pillars of the VA.	

OGC does not intend to share information in CG-E with any other VA offices. When OIT collects and processes data, the information is used to defend or prosecute lawsuits filed against or by the United States. In such cases, the information is used by the attorneys (VA and DOJ) who are assigned to the case. The attorney may discuss emails or MS Office files, for example, with the VA employees or other persons who are involved in the litigation. That is done through interviews and depositions with the persons who are relevant to the litigation.

**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:** Access to the application is restricted to OGC employees and to two application administrators from Infrastructure Operations. The privacy risk associated with transmitting SPI within the Department of Veterans’ Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

**Mitigation:** During the review process all privacy protected information that is protected by federal and state law that is not material to the litigation, such as SPI of a person not relevant to the litigation, would be redacted.

Access to the application is restricted to authorized VA employees and contractors which may include, but are not limited to: OGC, FOIA, and to application administrators from the VA.

## 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</i>	<i>List the purpose of information</i>	<i>List the specific PII/PHI data elements that are processed</i>	<i>List the legal authority,</i>	<i>List the method of transmission</i>
--	--	---	----------------------------------	--

<i>information is shared/received with</i>	<i>being shared / received / transmitted with the specified program office or IT system</i>	<i>(shared/received/transmitted)with the Program or IT system</i>	<i>binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>and the measures in place to secure data</i>
U.S. Department Of Justice	DOJ represents the DVA in all litigation	For each individual case, ESI collected for that case would be shared with the DOJ attorney who represents the United States in that case.	SORN 16VA026, reasonable use no. 10	Secure, encrypted portable hard drive.
Opposing parties and attorneys	Required by law; when a party is involved in a lawsuit the FRCP require that all relevant information be shared among the parties to allow the dispute to be resolved fairly.	For each individual case, ESI collected for that case would be shared with the private attorney who represents the party in that case. If the party has no attorney, then the information would be shared with the party directly.	FRCP	Either in native format (e.g., MS Word documents would be produced as electronic MS Word files) in another electronic format, such as PDF, or potentially as a load file for another e-discovery software platform.
Federal, State, Local and Tribal Judicial courts/tribunals	Required by law; when a party is involved in a lawsuit the FRCP require that all relevant information be shared among the parties to	For each individual case, ESI collected for that case would be shared with the private attorney who represents the party in that case. If the party has no attorney, then the information would be shared with the party directly.	FRCP	Either in native format (e.g., MS Word documents would be produced as electronic MS Word files) in another electronic

	allow the dispute to be resolved fairly.			format, such as PDF, or potentially as a load file for another e-discovery software platform.
--	--	--	--	---

**If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.**

In order to protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

**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:** The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran’s Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

**Mitigation:** As stated above, the Department of Justice represents the Department of Veterans Affairs in all litigation matters. All ESI collected and processed through Casepoint Government -E (CG-E) is collected for an actual case being litigated in federal court must be given to DOJ so that its

attorneys can review the information for relevancy to the litigation. Additionally, as stated previously, ESI is collected because it is required by law when one party files a lawsuit against another. Thus, DOJ or OGC is required by law to disclose relevant, unprivileged ESI to the parties to the lawsuit.

Information is transferred in secure, encrypted hard drives. Additionally, there are no electronic connections to external organizations or systems

## 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.*

Specific notice of a collection is not required, however, “custodians” (anyone who may have relevant information) would normally receive notice of the possibility that ESI may be collected from computers and accounts that they use. For example, in most OGC cases, the first step is to use CG-E to send a custodian a “litigation hold notice,” which is a document that describes the pending or anticipated litigation and the information that the custodian must retain that is relevant to the litigation. Not all litigation hold notices will result in the collection of ESI from each custodian. If it is determined that ESI must be collected from a custodian that is achieved through coordination with OIT. The custodian may be aware of the collection because of their involvement in the pending or anticipated litigation, but notice is not required.

**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*

A custodian may not decline to provide information, as all information is pulled from VA IT systems and devices.

All VA employees consent to the collection of their data on VA systems and devices.

### **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*

Consent to particular uses is not applicable. All data collected by CG-E is used for litigation.

### **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:** Not applicable, as notice is not required when collecting data for litigation. A custodian may not decline to provide information, as all information is pulled from VA IT systems and devices.

**Mitigation:** Not applicable, as notice is not required when collecting data for litigation. All ESI collected and processed through CG-E is collected for an actual case being litigated in court.

## 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.*

There is no requirement for users to be permitted to gain access to the information once it is imported into the CG-E system. The attorney-client privilege and attorney work-product rule allow for the confidentiality of attorney case files. As the information in CG-E is considered part of the case file, it is exempt from disclosure.

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

*Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.*

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

There is no requirement for the application or individuals to correct the information for accuracy. As stated previously, the purpose of the CG-E system is actually to preserve information exactly as it was kept in the normal course of VA operations, to review it and potentially to share it in its native format with other parties and the court, as required by law.

### 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.*

Not applicable. As stated above, data is to be collected and preserved in the exact state that it was maintained. In fact, if custodians were allowed to change the data that would be a violation of law for which the United States and VA could be sanctioned by a federal judge.

#### **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.*

Not applicable. As stated above, data is to be collected and preserved in the exact state that it was maintained. In fact, if custodians were allowed to change the data that would be a violation of law for which the United States and VA could be sanctioned by a federal judge.

#### **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:** Not applicable. As stated above, data is to be collected and preserved in the exact state that it was maintained.

**Mitigation:** Not applicable. As stated above, data is to be collected and preserved in the exact state that it was maintained.

## 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.*

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; This documentation and monitoring is performed through the use of TMS.

The access to the system is granted per request by OGC Information Law Group Chief Council. Both a supervisor of the employee requesting to open a case and an OGC E-discovery Program Manager (OEPM) must approve a request to open a new case. The access is granted to an individual attorney to the data scope identified by the OEPM.

The roles in the system are as follows:

- System administrator – complete access to the system and data
- Case Administrator's, Case Manager's, and Case Users can be customized. Options below can be granted or removed:

#### General Rights:

- Allow integrated analytics access
- Allow analysis tags dashboard access
- Allow access to management charts
- Allow reports access
- Allow mobile access

#### Document Access Rights:

- Allow viewing
- Allow tagging
- Allow move or removing from folders
- Allow bulk tagging
- Allow smart tagging
- Allow viewing of prediction ranks
- Allow predictive coding actions
- Allow access to tag event comments
- Allow access to item notes
- Allow redacting
- Prompt for reason code
- Allow tag history viewing
- Allow tag history searching
- Allow exporting
- Allow printing
- Allow native download
- Allow media streaming
- Allow caching for review
- Allow searching and filtering by processing flags

#### Case Administration Rights:

- Allow case status access
- Allow case processing source setup
- Allow user management
- Allow activity report access
- Allow group and topic management
- Allow tag definition
- Allow folder setup
- Allow folder check-out management
- Allow production folder management
- Allow unlocking of production folders after export
- Allow custodian management
- Allow participant management
- Allow viewing exceptions
- Allow managing exceptions

Allow OCR processing  
Allow image management

Additionally, access can be further modified per folder, per document and per identification tag group basis.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

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

OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter.

**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.*

Personnel that will be accessing VA information or VA information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. OGC employees must also complete annual Privacy and Security training.

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

*If Yes, provide:*

1. *The Security Plan Status,:* Casepoint Government -E (CG-E) SSP was submitted to VAOIT – Cyber Security team for A&A
2. *The Security Plan Status Date,:* Submitted 8/20/2021
3. *The Authorization Status,:* Waiting for authorization
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
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.*

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

## **Section 9 – Technology Usage**

The following questions are used to identify the technologies being used by the IT system or project.

### **9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

Yes. The System is FedRAMP Certified with Agency Authorization

Casepoint has chosen to adopt the principles established in NIST SP 800-53 Control Family guidelines, as the official policy for this domain. In accordance with FIPS Publication 199, “Standards for Security Categorization of Federal Information & Information System”, Casepoint has selected an overall MODERATE security categorization per the principles of Confidentiality, Integrity & Availability. **Identify the cloud model being utilized**

### **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.*

Casepoint Government -E (CG-E) is a web-based SaaS application hosted in the Microsoft Azure cloud (for IaaS & PaaS). Casepoint Government -E (CG-E) falls under the FedRAMP cloud deployment model: Government Only Community - Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations.

Contract # 47QSMA19D08NU includes several VA privacy clauses related to ownership rights over data including PII.

### **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.*

Casepoint has implemented real-time event monitoring, correlation, and alerting provided by a combination of [Azure-Services], and SIEM within the Casepoint environment. SIEM is configured to monitor all identity and access events (Access authentication points, Server end points, Azure and Application events) creating alerts to notify security personnel of events of interest (e.g., Use of default account, excessive failed login attempts, etc.). The central log data are compiled together by SIEM and is reviewed by the Security Manager. Casepoint's Security Team offers advice and assistance to users of the information system for the handling and reporting of security incidents. Any potential incidents can be reported to the Casepoint Security Team through email [networkstaff@casepoint.com](mailto:networkstaff@casepoint.com)

### **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.*

Casepoint's contract with VA includes FAR 52.227-14 Rights in Data-General

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

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

Not Applicable

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<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, Rita Grewal**

---

**Information System Security Officer, Scott Miller**

---

**Information System Owner, Michael Vella**

## 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).

Due to the nature of ligation systems the standard Notice of Privacy Practices is not required in accordance with FRCP.