## SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

*The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).*

VA HANDBOOK 6508: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=767&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

# QTC Communication Server

# Medical Disability Examination Program Office (MDEPO)

Date PIA submitted for review:

09/23/20

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Quanisha Jones | Quanisha.Jones@va.gov | 202-632-7114 |
| Information System Security Officer (ISSO) | Yolanda Maury | yolanda.maury@va.gov | 973-297-3352 |
| Information System Owner | Jennifer Treger | Jennifer.treger@va.gov | 202-461-9497 |

## Abstract

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

QTC Medical Services, Inc. (QTC) provides appointment scheduling, examinations and tracking for Veterans Benefits Administration (VBA) compensation and pension (C&P) program.
The QTC system supports coordination of contracted Medical Disability Examination (MDE) requests and the transmission of Disability Benefits Questionnaire (DBQ) results back to the Department of Veterans Affairs (VA). The system is not a cloud service provider; the system operates as a VA managed service provider external to all VA systems.

## 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.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *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?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

QTC stores, processes, and transmits MDE data between QTC (3 contracts covering all Regional Offices) and the VA information technology systems including Virtual VA, Data Access System (DAS), and Veterans Benefits Management System (VBMS).

MDEs for Decision Ready Claims: The VA Regional Office (VARO) employee requests a medical exam for Decision Ready Claims (DRC) through the Intranet web application, which generates a secure text file of the request, which is then securely forwarded to QTC.

MDEs for all claims other than DRC: The VARO employee requests a medical exam in VBMS which generates a transaction sent through DAS to the QTC system (which is referred to as Exam Management System (EMS)).

In addition and when indicated, QTC will obtain electronic medical records (also known as C-files) from VBMS that will be needed by the QTC medical examiners. All medical record files are segregated by individual Veteran, i.e. a single file of medical records per Veteran.

The medical examiners perform exams, capture the required information and send the results to QTC. QTC generates a report of the exam results using DBQ(s), which is electronically transferred to the appropriate VA system (DAS) from the QTC data center in Irvine, California, over a FIPS 140-2 secure connection.

The QTC system contains Veteran medical records that contain both Protected Health Information (PHI) and Personally Identifiable Information (PII) data. The system interconnection described in this Privacy Impact Assessment (PIA) may enable the transmittal of both VA owned sensitive information and non-VA owned sensitive information as well as non-sensitive information, depending on the business needs described in this document. Sensitive information types are discussed in 1.1. Regardless of which entity owns the information, if VA transmits sensitive information to QTC, through the system interconnection, the transmission must be protected through the use of FIPS 140-2 (or successor) validated encryption.

QTC's primary data center is securely housed in a Statement on Standards for Attestation Engagements No. 16 (SSAE 16) certified Tier 4 Data Center under a managed services contract with AT&T.

Redundant equipment that stores VA data information is located at the AT&T Data Center in Irvine, CA. The Data Center operates 24/7 and provides continuous monitoring of computer systems, applications, client data and networking infrastructure. Access to Data Center facility is controlled by guard station sign-in and mantrap biometrically secured doors. This building has a Facilities Protection Procedure manual that provides guidelines on managing a wide variety of events including but not limited to; adverse weather conditions, handling bomb threats, and fires.

The QTC system serves and supports approximately 300k Veteran exam requests per year through the coordination of contracted Medical Disability Examination requests and the transmission of DBQ results back to the VA. The system is not a cloud service provider. The system operates as a VA managed service provider and is required to comply with all applicable VA and federal information security requirements for a managed service provider.

PII is used internally, and shared externally, only for the authorized purposes identified in its public notices, and as authorized in System of Records Notice (SORN) 58VA 21/22/28. Authority For Maintenance Of The System: Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C.,section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55. In addition, QTC enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements.

The SSN is used for purposes of Veteran Identification and verification.

QTC documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. It further conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

The risks associated with the disclosure of PII/PHI information can result in harm to an individual whose privacy has been breached.

## Section 1. Characterization of the Information

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

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

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

*If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.*
*This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.*

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

☒ Name
☒ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☐ Personal Phone Number(s)

☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Other Unique Identifying Number (list below)

The data transmitted via DAS is owned by VBA contains PII and PHI data as listed below: • Medical Information • Veteran Account Number • Veteran Diagnosis Summary • Physician Name • Physician License Number

**PII Mapping of Components**

**QTC Communication Server** consists of 1 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **QTC Communication Server** and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

*PII Mapped to Components*

| **Components of the information system (servers) 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** |
|---|---|---|---|---|---|
| VA ExamTrack | Yes | **No** | Veteran Name<br>Veteran SS#<br>Veteran Account Number<br>Veteran Diagnosis Summary<br>Physician Name<br>Physician License Number | Supports coordination of Contract Exam requests and the transmission of DBQ results back to the VA | FIPS 140-2 Data encryption in transit and at rest |

### 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.*

The Veterans' Benefits Management System (VBMS) is a centralized Web-based application written in Java with multiple open source, commercial, and custom components. Users access VBMS through a web-browser through the VA Wide Area Network.

The interconnection between the VA systems and QTC Communications Server, owned by QTC Medical Services, Inc., is a two-way path. For sensitive information, no user services are offered. QTC will not require access to VA systems. VA employees will require logon access to the QTC system. All access to VA files is managed by QTC. The various work flows include:

- The transmission in both directions is a "system-to-system" exchange of PII and PHI between QTC, and the VA IT systems. Only exam requests described above are passed to QTC from the VA. The exam requests are converted to a .pdf file format and encrypted before they are sent out. The exam requests are stored in a secure folder at QTC. On the other end of the connection, QTC will protect the exam reports using Secure Hash Algorithm 2 Advanced Encryption Standard (SHA2 AES) certificate-based encryption and place the exams in a secure folder on the communication server.

- **DAS (from VBMS, owned by VBA) – Used for all Claims other than DRC**

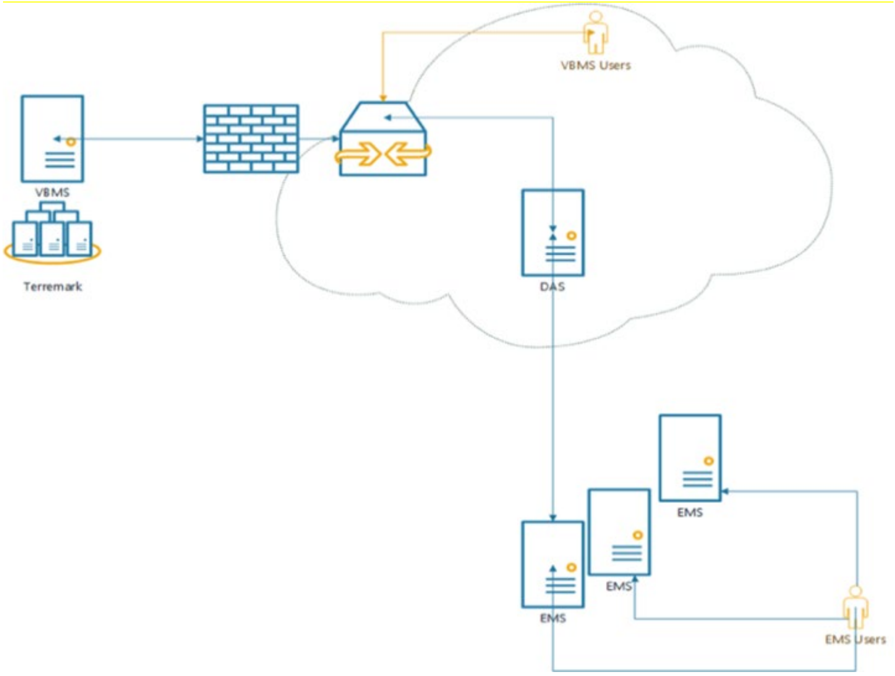
  **– System Name**
  Data Access System (DAS) is the interface between QTC and Veterans Benefits Management System (VBMS)

  **– Function:** VBMS is a web-based, electronic claims processing solution complemented by improved business processes. VBMS is part of the VA larger organizational transformation effort. Implementation of VBMS is helping VA meet increasing demand while providing more timely and responsive customer service to Veterans, Service Members, and their families. VBMS is currently assisting in eliminating the existing claims backlog and, once fully developed and deployed, will serve as the enabling technology for quicker, more accurate, and integrated claims processing.

  **– Location**
  Verizon (formerly Terremark) Network Access Point of the Capital Region (NAP)

VBMS is used to request exams via Data Access System (DAS) which sends the requests to the contractor's Exam Management System (EMS).

This integration uses bidirectional communication between DAS, and EMS, where EMS system or systems may expand over time. The goal of this architecture (see figure below) is to create a reusable technical infrastructure, message flow and data model that can be leveraged by future vendors with minimal to no modification to existing systems.



*Communication Architecture*

QTC generates a report of the exam results, which is then transferred electronically to the appropriate VA system from the QTC contractor site in Irvine, California, over a FIPS 140-2 secure connection. The "round-trip" process involves the VARO logging in to request the exam, and then monitoring VA systems to determine when the results are available. The data to be transmitted from QTC includes Federal Information Processing Standard (FIPS) 199 sensitivity categorization level.

**System Sources of Information**

- **The QTC Communications Server, owned by QTC.** QTC, A Leidos Company

  **– Name**
  QTC Communication Server

  **– Function**
  QTC provides a secure folder on their Communication Server located behind their firewall in which medical exam requests from VA and supporting documentation, are obtained from VBMS via DAS. This site is accessible to QTC employees with limited access rights.

  **– Location**

QTC Data Center

This system contains Veteran medical records that contain both PHI and PII data. The system interconnection described in this Privacy Impact Assessment may enable the transmittal of both VA owned sensitive information and non-VA owned sensitive information as well as non-sensitive information, depending on the business needs described in this document. Sensitive information types are discussed in Appendix D.

Regardless of which entity owns the information, if VA transmits sensitive information to QTC, through the system interconnection, the transmission must be protected through the use of FIPS 140-2 (or successor) validated encryption.

### 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.*

For all claims other than DRC:
VBMS Exam Management System (EMS) is used to request exams via Data Access Service (DAS) which sends the requests to the contractor's Exam Management System (EMS).a web-based, electronic claims processing solution for data collected by VBA on claims submissions by the examinee (Veteran).

### 1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

*Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.*

*If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.*
*This question is related to privacy control AP-2, Purpose Specification.*

The QTC System supports coordination of contracted MDE requests and the transmission of DBQ results back to the VA to support claims adjudication. This information is used to support claims adjudication for examinees (Veterans) who have filed a disability claim

### 1.5 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.*

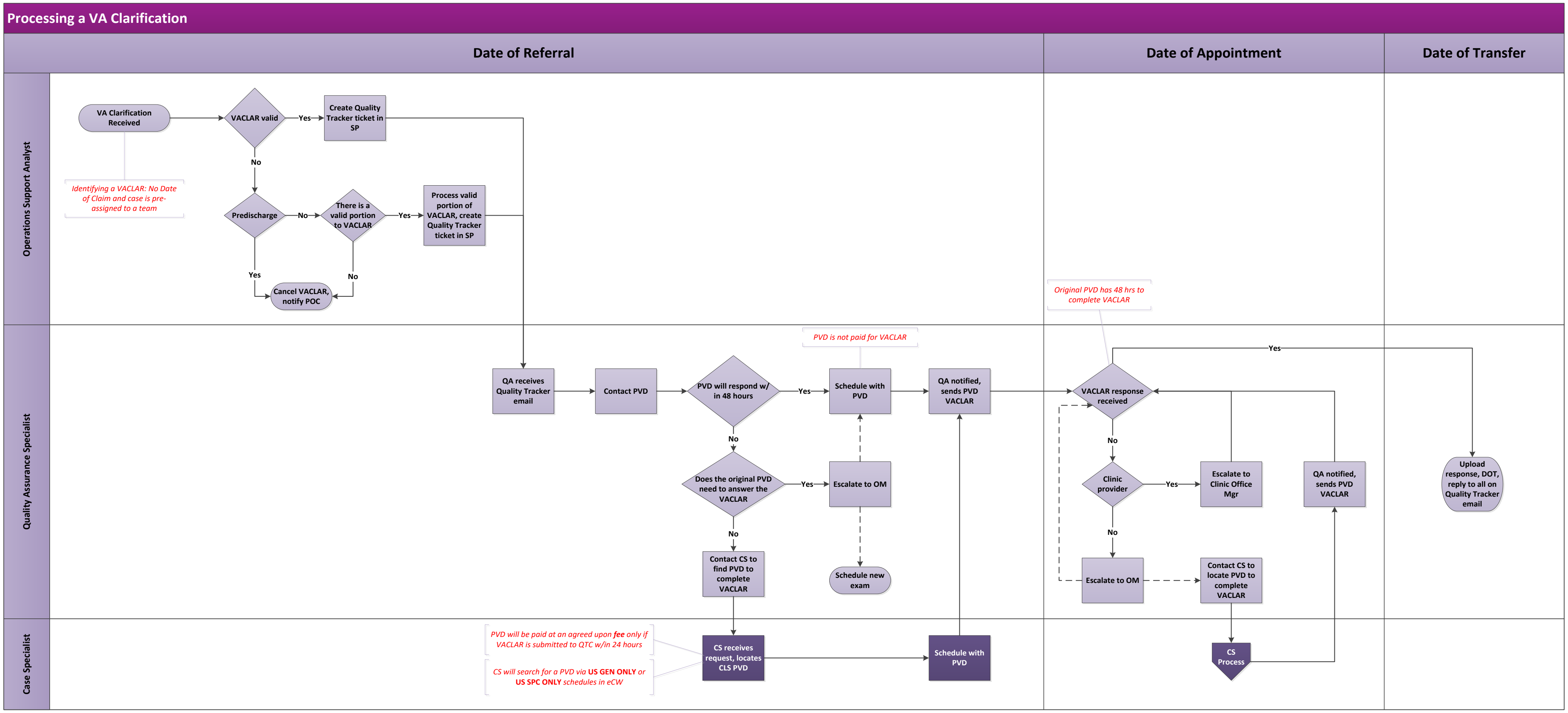
To protect the integrity and quality of the PII it collects or otherwise maintains, QTC issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. It documents processes to ensure the integrity of PII through existing security controls, and confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.

Upon receiving an Insufficient or Inadequate request from the VA an Operations Support Analyst (OSA) will determine whether a Clarification Request is required:

- The OSA will review the request and any pertinent information to determine the validity of the request on Date of Referral (DOR)
- If the VA Clarification is determined to be valid, the OSA will create a Quality Tracker ticket in SharePoint on DOR
- If the entire VA Clarification is not valid, the OSA will cancel the request
- For Compensation and Pension (CNP), the OSA will process the valid portion of the VA Clarification and create a Quality Tracker ticket in SharePoint on DOR
- For Pre-Discharge, any portion of the VA Clarification that is not valid results in the OSA cancelling the entire request. OSA will notify the POC via email separately

The Quality Assurance Specialist (QAS) will provide all pertinent information to the original or Medical Opinion/Medical Record Review (MO/MRR) only provider including but not limited to the report requiring clarification and clarifying questions. The original and IMO/MRR only providers will be contacted by the QAS if a response is not received within 48 hours from the DOR.

VA Clarification responses received will be uploaded and tracked in eProcess to Pre-Delivery Check (PDCK) and/or Date of Transfer (DOT). The process for a VA Clarification Request can be seen in workflow below.


Processing a VA Clarification
Date of Referral
Date of Appointment
Date of Transfer
Operations Support Analyst
Quality Assurance Specialist
Case Specialist
VA Clarification Received
Identifying a VACLAR: No Date of Claim and case is pre-assigned to a team
VACLAR valid
Yes
Create Quality Tracker ticket in SP
No
Predischarge
No
There is a valid portion to VACLAR
Yes
Process valid portion of VACLAR, create Quality Tracker ticket in SP
Yes
No
Cancel VACLAR, notify POC
QA receives Quality Tracker email
Contact PVD
PVD will respond w/ in 48 hours
Yes
PVD is not paid for VACLAR
Schedule with PVD
QA notified, sends PVD VACLAR
No
Does the original PVD need to answer the VACLAR
Yes
Escalate to OM
Schedule new exam
No
Contact CS to find PVD to complete VACLAR
PVD will be paid at an agreed upon fee only if VACLAR is submitted to QTC w/in 24 hours
CS will search for a PVD via US GEN ONLY or US SPC ONLY schedules in eCW
CS receives request, locates CLS PVD
Schedule with PVD
Original PVD has 48 hrs to complete VACLAR
Yes
VACLAR response received
No
Clinic provider
Yes
Escalate to Clinic Office Mgr
QA notified, sends PVD VACLAR
No
Escalate to OM
Contact CS to locate PVD to complete VACLAR
CS Process
Upload response, DOT, reply to all on Quality Tracker email

*Process Workflow*

VA will apply direction in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes.

Individuals may appeal an adverse decision and have incorrect information amended, where appropriate. The VA shall have ultimate oversight, review, and rejection/acceptance for all deliverables, tasks, and sub-tasks related to this program/acquisition.

### 1.6 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*

QTC determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

QTC also describes, in its privacy notices, the purposes for which PII is collected, used, maintained, and shared. SORN 58VA 21/22/28 outlines that the SSN is used for purposes of Veteran Identification and verification, and may be used for disability eligibility determination.

The authority governing VA for this interconnection is based on: AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C.,section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51.

- Federal Information Security Management Act (FISMA)
- VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*, and Handbook 6500, *Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program*
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran’s Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

Authority for Department of Veterans Affairs (VA) VLER and Data Access Services (DAS) to share data for the purpose outlined under this Agreement with the recipient is as follows: DAS.

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended

- VA Claims Confidentiality Statute, 38 U.S.C § 5701
- HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
- Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. § 5705
- Freedom of Information Act (FOIA), 5 U.S.C. § 552

### 1.7 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

*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:*

*<u>Principle of Purpose Specification:</u> Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?*

*<u>Principle of Individual Participation:</u> Does the program, to the extent possible and practical, collect information directly from the individual?*

*<u>Principle of Data Quality and Integrity:</u> 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:
**<u>Privacy Risk:</u>** The risks associated with the disclosure of PII/PHI information can result in harm to an individual whose privacy has been breached.

Inappropriate internal sharing and disclosure:

- Viewing a relatives information
- Viewing a co-workers information
- Viewing their own records

**Mitigation:** QTC provides employee/staff with security training needed to support QTC security policies and procedures in the course of their normal work.

The QTC security training and awareness program consists of security awareness presentations, security reminders, general security training, system-specific security training, security management training and professional security education for members of the workforce.

All new members of the workforce will receive training orientation within a reasonable period of time after the member joins the organization.

All QTC workforce members receive continuing information security and privacy awareness updates that focus attention on security issues to ensure the workforce is up-to-date with new threats, such as computer viruses, spyware, social engineering attacks, and other issues that may compromise the confidentiality, integrity, and availability of ePHI.

## 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.*

*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.*

- Full Name: Veteran's identification
- Social Security Number: Used to verify Veteran identity
- Medical Information: Used to track medical information
- Account Number: Used as reference for the Veteran's account
- Physician Name : Used to identify the doctor
- Physician License Number: Used to verify doctors identity
- Zip code
- Diagnosis Summary
- Email
- Financial Account Information
- Health Insurance Beneficiary Number

The information in the system will be used to schedule Compensation and Pension examinations as well as supply the VA the results of the examination via a DBQ(s).

**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*

QTC generates a report of the exam results, which is then transferred electronically to the appropriate VA system from the QTC data center in Irvine, California, over a FIPS 140-2 secure connection. The "round-trip" process involves the VARO logging in to request the exam, and then monitoring VA systems to determine when the results are available.

The QTC system itself does not perform any kind of analysis or run analytic tasks in the background. QTC understands the importance of minimizing, to the extent it is able, and the data it collects. To that end, it:

- Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
- Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;
- Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose;
- Locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure and;
- Develops policies and procedures that minimize the use of PII for testing and/or training; and implements controls to protect PII used for testing and/or training.

**2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access**

**documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

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

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

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

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

The SORN (58VA21/22/28) defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is to support the individual claim or claims the Veteran has been granted.

QTC grants access to information systems based on a valid need-to-know that is determined by assigned official duties.

Managers/supervisors must submit a request to grant access to information systems based on a valid need-to-know that is determined by assigned official duties that satisfy all personnel security criteria and intended system usage.

The manger/supervisor responsible for the user will determine the appropriate menus, when applicable. The supervisor will also determine any other programs or access required by the user. Responsibility and authorization for the creation or modification of application menus and system access within the systems is under the control of the Information System Owner, local CIO, or designee.

The security controls for the QTC application cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.

The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

The QTC application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected." Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security, and have signed VA Rules of Behavior.

## 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*

The following information is retained:

- Full Name
- Social Security Number
- Mailing Address

**3.2 How long is information retained?**

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.*

*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.*

Specific retention timelines and destruction/disposal requirements are based on QTC's contract with the VA.

- **Functional Acquisition Regulation (FAR) 52.212-5** --- related extract regarding record retention:

  The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

- **Performance Work Statement (PWS) Section:**

  Prior to termination or completion of this contract, Contractor will not destroy information received from VA or gathered or created by the Contractor in the course of performing this contract without prior written approval by the CO. A Contractor destroying data on VA's behalf must do so accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, and applicable VA Records Control Schedules. All data and reports shall be transferred to VBA upon contract completion. For Medical Record/Case History retention is for the current contract end of term (or completion of last Medical Exam) plus 13 months. For Accounts Receivable Financial records, are kept for the current contract end of term plus 10 years or receipt of la AR payment.

### 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.*

These records are retained and disposed of in accordance with the General Records Schedule 3.2: Information Systems Security Records, approved by National Archives and Records Administration. Records are maintained according to (VBA RCS) (VB-1) (VB-2).

### 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*

Records/digital information will be eliminated following the sanitization procedures in VA Handbook 6300.1 Records Management Procedures and VA Directive 6500 VA Cybersecurity Program. Paper Records are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

Specific retention timelines and destruction/disposal requirements are based on Statute of limitations for Government Claims as documented in QTC/Client contracts and the QTC FOR-QIT-Data Retention Log (Refer to table below for details). The QTC/Client contracts' are maintained and updated by the Accounting/Financial department and Corporate Internal Audit. The QTC FOR-QIT-Data Retention Log is audited and maintained by QTC IT Services.

Iron Mountain is the designated data storage service vendor. Iron Mountain does not destroy or scratch any tapes. QTC tapes remain securely stored until recalled and/or recycled for use. Director QIT must review and approve the tape recall/recycle action.

- Daily: The QTC System is backed-up nightly (Daily) to tape & disk via CommVault.

- Weekly: QTC maintains and rotates three (3) weeks of backups.

- Monthly: Month-End Tapes: At month-end, backups are created on a different set of tapes And sent off-site to Iron Mountain storage and security facility.

- Annual/Yearly: Month-End Tapes rotate up to an annual tape
- One (1) year = Twelve (12) End-of-Month Tapes.
- Year-end tape retention period: 5/15/09, QTC retention period revised to 10 Yrs. Plus (+) Contract End – Date or receipt of last AR payment (Default to latest date).

Backup media is accounted for and version controlled from creation through storage and transportation and recycling or destruction. QTC uses CommVault Enterprise backup software to backup all QTC financial data nightly to disk then it is backed up to a tape and moved to an off-site Iron Mountain tape vault on end of month tapes (EOM). In order to ensure that all data is protected appropriately we first ensure that the media has the data labeled correctly.

All backup sets and individual tapes are catalogued within CommVault, all tapes are 100% encrypted. The media, whatever it is, will be appropriately labeled externally so that it is visible when the media is handled Tapes are bar coded to identify them within the backup sets, tape library and tape vaulting systems. Tapes are transported via locked tape box from data center to the Iron Mountain tape vaulting facility.

Other retention periods include:

| *TYPE OF RECORD | RETENTION PERIOD | STORAGE SOURCE |
|---|---|---|
| Medical Record/Case History | Current Contract End – of – Term (Or completion of last Medical Exam) + Thirteen (13) Months | o Tracking Tool and ExamTrack<br>o Tape Back-up |
| Accounts Receivable Financial Records<br>E-Mail | *Current Contract End – of – Term + Ten (10) Years or Receipt of last AR payment (Default to latest date). | o Billing data maintained via Tracking Tool.<br>o Annual Tape Back-up: 10 years*<br>o QTC/IM contract maintained by Accounting & Finance Dept. |

| *TYPE OF RECORD | RETENTION PERIOD | STORAGE SOURCE |
|---|---|---|
| | | o CommVault Archiving |

**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*

QTC does not use or disclose PHI for purposes not otherwise provided for by the Customer (Covered Entity) without obtaining a written authorization from the Covered Entity (VA). All uses and disclosures of PHI is made pursuant to a signed authorization and must be consistent with the terms and conditions of the authorization. QTC's policy to access, obtain, use and disclose de-identified information, rather than PHI, in instances when the need may arise or when appropriate and consistent with business and legal requirements. Health information that has not been de-identified in accordance with all applicable state and federal laws shall be considered confidential and shall not be accessed, obtained, used or disclosed by QTC.

QTC will not de-identify PHI for its own purposes unless specifically permitted by the Customer (Covered Entity). Any employees found to have violated PHI disclosure provisions will be disciplined in accordance with QTC policy up to and including termination of employment. The type of sanction will depend on the intent of the individual and severity of the violation.

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

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

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

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

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

*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:** There is a risk that the information maintained by QTC could be retained for longer than
is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** To mitigate the risk posed by information retention, QTC adheres to the NARA General Records Schedule 3.2, VB-1, and VB-2 approved by National Archives and Records Administration (NARA) https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf

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

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

**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?**

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Data Access System (DAS) | DAS is the common service that exchanges information with other agencies both within VA and external to VA | Full name; Social Security Number; Taxpayer identification number; Street address; email address; medical information | SOAP over HTTPS using SSL encryption and Certificate Exchange |

## 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:** The risks associated with the disclosure of PII/PHI information can result in harm to an individual whose privacy has been breached. The list below outlines some of these risks:

- Medical / Identity Theft
- Disclosure of Genetic Information for Underwriting purposes
- Sale of Protected Health Information
- Medical Fraud

**Mitigation:** QTC provides employee/staff with security training needed to support QTC security policies and procedures in the course of their normal work.

The QTC security training and awareness program consists of security awareness presentations, security reminders, general security training, system-specific security training, security management training and professional security education for members of the workforce.

All new members of the workforce will receive training orientation within a reasonable period of time after the member joins the organization.

All QTC workforce members receive continuing information security and privacy awareness updates that focus attention on security issues to ensure the workforce is up-to-date with new threats, such as computer viruses, spyware, social engineering attacks, and other issues that may compromise the confidentiality, integrity, and availability of ePHI.

## 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: This question is #7 in the Privacy Threshold Analysis.**

*Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

*For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.*

*What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?*

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing with Third Parties*

*Data Shared with External Organizations*

| ***List External Program Office or IT System information is shared/received with*** | ***List the purpose of information being shared / received / transmitted with the specified program office or IT system*** | ***List the specific data element types such as PII/PHI that are shared/received with the Program or IT system*** | ***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|
| QTC | Information is shared with QTC so QTC can assign requests for medical disability examinations (MDEs) to private contracted doctors. The MDE's are used by VA in support of Veteran compensation and pension claims. | • Veteran Name<br>• Veteran Social Security Number<br>• Veteran Account Number<br>• Veteran Diagnosis Summary<br>• Physician Name<br>• Physician License Number | AUTHORITY FOR MAINTENANCE OF THE SYSTEM:<br>Title 10 U.S.C. chapters 106a, 510,<br>1606 and 1607 and Title 38, U.S.C.,<br>section 501(a) and Chapters 11, 13, 15,<br>18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,<br>53, and 55.<br>SORN 58 VA 21/22/28<br>VLER DAS MOU & ISA | Transmitted from VA to QTC Results received back at VA through DAS. FIPS 140-2 encryption is used to secure data during transmission in both directions. |
| Iron Mountain | All system data is encrypted for back-up and provided to Iron Mountain in case recovery is required. | Full name;<br>SSN;<br>Street address;<br>Email address;<br>Telephone number(s);<br>Date of Appointment (DOA);<br>Provider name;<br>Provider Street address;<br>Disability Benefits Questionnaires; | Data Storage and Service Agreement # 190-2820 | All system data is encrypted for back-up and provided to Iron Mountain in case recovery is required. |

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

QTC shares the information with contract doctors in accordance with System of Records Notice (SORN) 58VA 21/22/28 Authority for maintenance of the system: Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C.,section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55. 58VA21/22/28in support of Veteran medical disability examinations.

The SSN is used for purposes of Veteran Identification and verification, and may be used for disability eligibility determination.

QTC documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. It further conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

QTC implements the following security measures and controls:

- Patch management policy - QTC utilizes automated patch management to keep all QTC IT equipment patched with the latest operating system and application updates. Reports are run regularly and remediation is implemented for devices missing patches.
- Malware prevention / Virus Scanning policy - Every QTC managed internal system has antivirus and antispyware software installed, and is monitored 24x7 for new infections. Management is centralized. Updates are done daily, or more frequently, if necessary.
- Audit policy - QTC regularly audits the security controls (continuous monitoring) and compliancy towards QTC policies. Plan of Action and Milestones are used to track deficiencies and remediation.
- Incident response / security breach notification policy - QTC maintains a Computer Incident Response Team and network activity is monitored 24x7.
- User certification, identification and authentication policy - User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. QTC utilizes 2 factor authentication for all general users.
- Password policy - QTC requires a strong password and users must change their password every 60 days.
- Account Management policy - QTC accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every 90 days. QTC policy requires account termination within 24 hour of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination.
- Physical and environmental security policy - Physical and environmental controls are maintained at each QTC facility. Badges are required for all employees and contract staff. QTC computer rooms are environmentally controlled for operation of the equipment is contains. This includes power, network, HVAC, and fire suppression.

- Firewall, IDS, and encryption policy - Intrusion detection systems (IDS). IDS are in place at all gateways and throughout the QTC network. The QTC network is monitored 24x7. Suspicious activity is reviewed and as needed recommendations are formulated and assigned to the system administrators. FIPS 140-2 encryption is required for transmission of sensitive information.
- Contingency Plans - A contingency and disaster recovery plan is in place for every QTC IT system. The plans are tested regularly based on the criticality level.

### 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 risks associated with the disclosure of PII/PHI information can result in harm to an individual whose privacy has been breached.

Inappropriate external sharing and disclosure:

- Viewing a relatives information
- Viewing a co-workers information
- Viewing their own records

**Mitigation:** QTC shall take corrective action when examination deficiencies are identified and return any corrective/additional information to the VA within 14 calendar days of identification of the deficiency.

The VA shall have ultimate oversight, review, and rejection/acceptance for all deliverables, tasks, and sub-tasks related to this program/acquisition.

As a preliminary risk assessment, QTC shall ensure that all systems and data that fall under the guidelines as stated in POL-ITSERV-Security Planning Policy have been categorized in accordance with FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems* and FIPS 200, *Minimum Security Requirements for Federal Information and Information 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.*

The authority to collect PII is documented in the System of Records Notice Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 34, 35, 36, 39, 51, 53, 55. The VA describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

QTC provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of their PII prior to its collection. It also provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of their PII.

QTC/VA provides notice of information collection in several ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additional notice is provided via the Notice of Privacy Practices

The Department of Veterans Affairs provides additional notice of this system by publishing System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 58VA 21/22/28, in the Federal Register and online. An online copy of the SORN can be found at:

   https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

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

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

Yes, Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)). This is handled by the VA, it is outside the scope of this contract, and not administered by SMSIS, but SMSIS abides by directions from VBMS.

Depending on the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. VA consent mechanisms include a discussion of the consequences to individuals for failure to provide PII

**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*

According to *VA Handbook 6500* QTC may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow VA to collect or use PII. In contrast, opt-out requires individuals to take action to prevent the collection or use of such PII. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending on the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. VA consent mechanisms include a discussion of the consequences to individuals for failure to provide PII.

Before collecting PII in connection with an information system or program, VA determines whether the collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII as well as the use of information collected is documented in the System of Records Notice (SORN), Privacy Act Statement and PIAs. In addition, the individual has the right to consent as outlined within the System of Records Notice (SORN). All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA address outlined.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

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

Follow the format below:
**Privacy Risk:** There is a risk that veterans and other members of the public will not know that QTC exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

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

## Section 7. Access, Redress, and Correction

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

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

*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.*

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, the Regional Office Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

**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.*

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

**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.*

The procedure for correcting information is outlined in this PIA, and SORN 58 VA 21/22/28. Formal redress is provided. All information correction must be taken via the Amendment process. This is handled by the VA, it is outside the scope of this contract, and not administered by QTC.

**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.*

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

Formal redress is provided. All information correction must be taken via the Amendment process. In addition, the individual may contact any Regional Office for guidance on how to gain access to his or her records and seek corrective action through the Amendment process. This is handled by the VA, it is outside the scope of this contract for administration by QTC.

**7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>**

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

*<u>Principle of Individual Participation:</u> 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?*

*<u>Principle of Individual Participation:</u> 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:
**<u>Privacy Risk:</u>** The individual may not be aware of how to access, redress or correct their information.

**<u>Mitigation:</u>** The procedures to correct or amend information is included in the applicable SORN 58 VA 21/22/28, and this PIA.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

## 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.*

QTC protects data privacy from unauthorized use or disclosure by its contractors and service providers by establishing privacy roles, responsibilities, and access requirements for such entities. QTC also includes privacy requirements in contracts and other acquisition-related documents.

QTC monitors and audits privacy controls and internal privacy policies on a regular and continuous basis to ensure effective implementation. Additionally, it designs information systems to support privacy by automating privacy controls.

All QTC production applications & systems are maintained by QTC's IT Infrastructure group. As part of QTC's System Development Life Cycle (SDLC) & IT Systems Management processes all changes to the QTC production systems are reviewed, tested and documented in QTC's IT Team Foundation Server (TFS) & SharePoint systems and include:

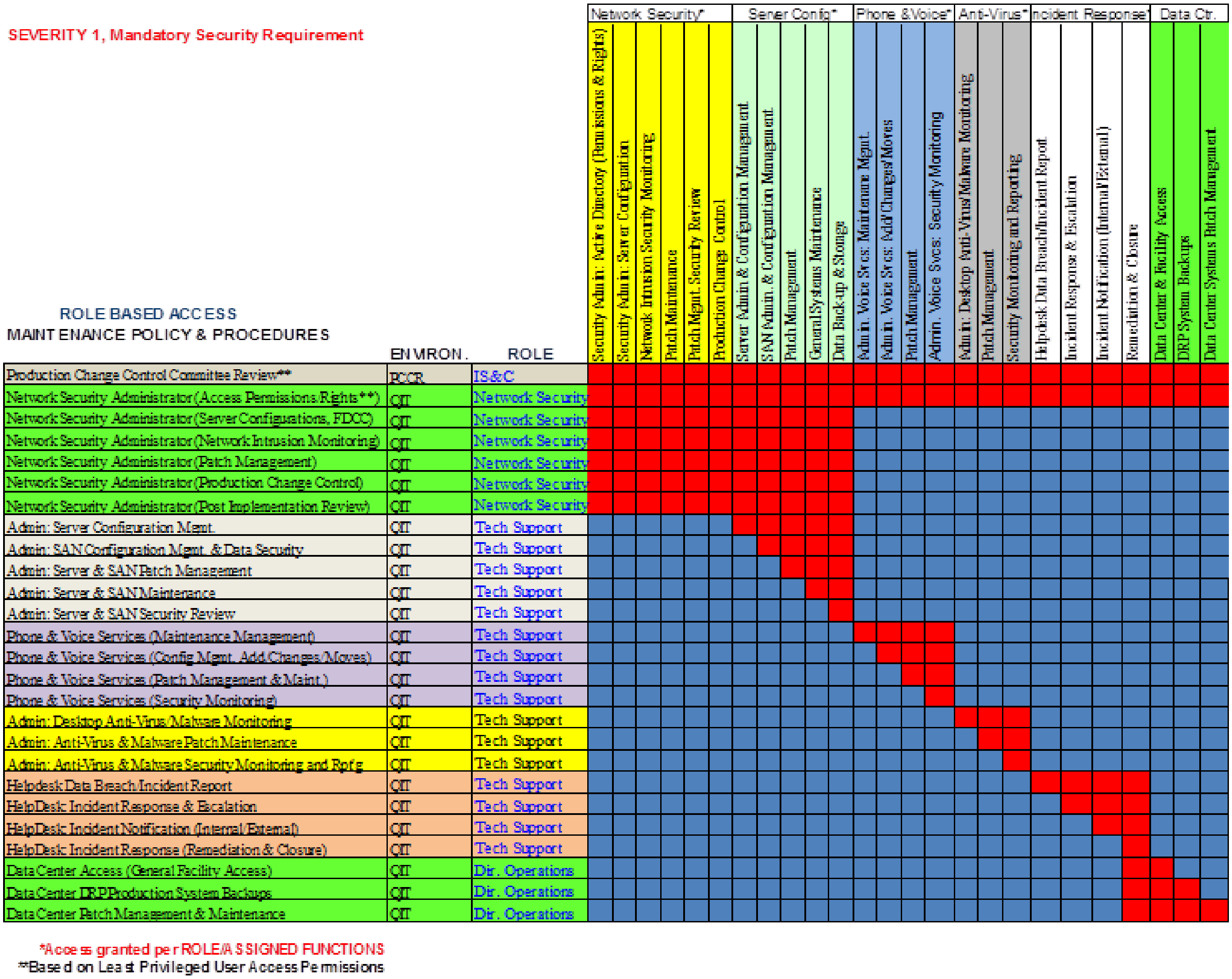
- Log and audit standards:
- Log and Audit messages contain at a minimum:
- Unique timestamp
- System name
- User or daemon where applicable

- Resulting message

For Basic Systems, periodic sampling, or spot checks will be used to review system logs and access reports.

- Group Policy for Windows systems in the QTC Active Directory (AD) are set to enforce specific event logs and audit settings.
- Critical systems logs are collected and presented to the support team and administrators via centralized syslog incorporated into the Application & System Monitoring tools.
- Security logging is performed in the multi-level antivirus/spam/malicious code scanning systems as well as in the MS AD event logging systems.
- Separation of Duties Security Guidelines identify the roles based duties and elevated privileges granted to accomplish the required software development and administrative tasks per QTC's security standards.

The figure below shows QTC's role-based access structure.



SEVERITY 1, Mandatory Security Requirement

ROLE BASED ACCESS
MAINTENANCE POLICY & PROCEDURES

| | ENVIRON. | ROLE | Network Security* | | | | | | Server Config* | | | | | Phone & Voice* | | | | Anti-Virus* | | | Incident Response* | | | | Data Ctr. | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Security Admin: Active Directory (Permissions & Rights) | Security Admin: Server Configuration | Network Intrusion Security Monitoring | Patch Maintenance | Patch Mgmt. Security Review | Production Change Control | Server Admin & Configuration Management | SAN Admin. & Configuration Management | Patch Management | General Systems Maintenance | Data Back-up & Storage | Admin. Voice Svcs: Maintenance Mgmt. | Admin. Voice Svcs: Add/Changes/Moves | Patch Management | Admin. Voice Svcs: Security Monitoring | Admin: Desktop Anti-Virus/Malware Monitoring | Patch Management | Security Monitoring and Reporting | Helpdesk Data Breach/Incident Report | Incident Response & Escalation | Incident Notification (Internal/External) | Remediation & Closure | Data Center & Facility Access | DRP System Backups | Data Center Systems Patch Management |
| Production Change Control Committee Review** | PCCR | IS&C | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 |
| Network Security Administrator (Access Permissions/Rights**) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 |
| Network Security Administrator (Server Configuations, FDCC) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Network Security Administrator (Network Intrusion Monitoring) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Network Security Administrator (Patch Management) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Network Security Administrator (Production Change Control) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Network Security Administrator (Post Implementation Review) | OIT | Network Security | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Server Configuration Mgmt. | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: SAN Configuration Mgmt. & Data Security | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Server & SAN Patch Management | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Server & SAN Maintenance | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Server & SAN Security Review | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Phone & Voice Services (Maintenance Management) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Phone & Voice Services (Config Mgmt. Add/Changes/Moves) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Phone & Voice Services (Patch Management & Maint.) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Phone & Voice Services (Security Monitoring) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Desktop Anti-Virus/Malware Monitoring | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Anti-Virus & Malware Patch Maintenance | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Admin: Anti-Virus & Malware Security Monitoring and Rpt'g | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Helpdesk Data Breach/Incident Report | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 |
| HelpDesk Incident Response & Escalation | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 |
| HelpDesk Incident Notification (Internal/External) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟦 | 🟦 | 🟦 |
| HelpDesk Incident Response (Remediation & Closure) | OIT | Tech Support | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 |
| Data Center Access (General Facility Access) | OIT | Dir. Operations | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟦 | 🟦 |
| Data Center DRP Production System Backups | OIT | Dir. Operations | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟦 |
| Data Center Patch Management & Maintenance | OIT | Dir. Operations | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 |

*Access granted per ROLE/ASSIGNED FUNCTIONS
**Based on Least Privileged User Access Permissions

*Role Structure*

**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 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.*

The Contracting Officer (CO) and Contracting Officer's Representative (COR) along with the program office perform monthly reviews of the contract. Access is a requirement of the contract, and employees require NACI clearance. The scope of the contract is to perform medical disability examinations and requires direct communication with veterans.

All QTC Privileged Contractor User accounts must sign the Privileged User/Super User (Contractor) acknowledgment. QTC Privileged Contractor User accounts are issued for a "Specified Time-Period based on Project and/or Task assignment". The Director, IT Operations, must approve the purpose and duties for "Privileged User" status. At the expiration of this period the Privileged Contractor User account will be de-activated be De-activated".

When a QTC Contractor and/or Service Provider is required to design, develop, operate, and/or maintain a system of a client's Medical Information and/or any PII records, this information must be safeguarded in compliance with Federal, State, and QTC Data Privacy Security Policies.

Service Contractor and/or Service Provider understand and agree they are responsible for the protection of claimant information entrusted to them, including the use and disclosure by persons directly employed or subcontracted by the provider.

Any agreement with the Contractor and/or Service Provider is fully incorporated into the **"AGREEMENT BETWEEN INDEPENDENT CONTRACTOR AND QTC MEDICAL GROUP, INC."** entered into by the Provider which states the Provider shall comply with the Privacy Act of 1974, Public Law 93-579 and all applicable state laws regarding privacy and protection of Claimant Information.

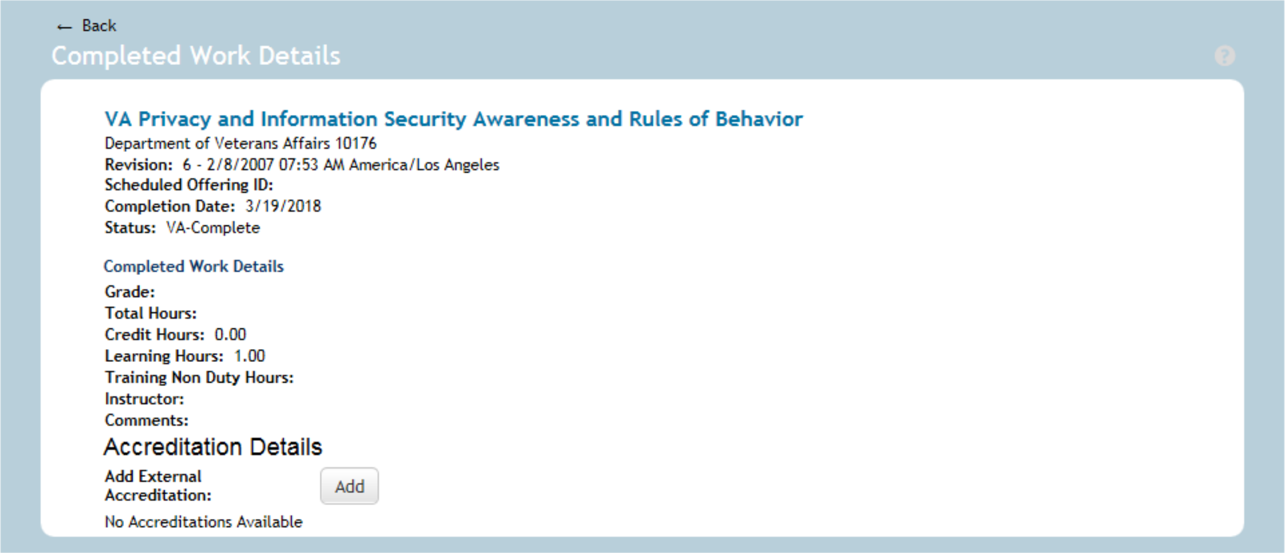
### 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

*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.*

QTC has developed and implemented a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. This training:

- Is administered at least annually and targets personnel having responsibility for PII or for activities that involve PII; and
- Requires personnel to certify acceptance of responsibilities for QTC privacy requirements.

QTC personnel are required to take VA annual Privacy and Information Security Training as seen in the example below:



VA Privacy and Information Security Awareness and Rules of Behavior
Department of Veterans Affairs 10176
**Revision:** 6 - 2/8/2007 07:53 AM America/Los Angeles
**Scheduled Offering ID:**
**Completion Date:** 3/19/2018
**Status:** VA-Complete

Completed Work Details
**Grade:**
**Total Hours:**
**Credit Hours:** 0.00
**Learning Hours:** 1.00
**Training Non Duty Hours:**
**Instructor:**
**Comments:**

Accreditation Details
**Add External Accreditation:**

No Accreditations Available

*Training Example*

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

*If Yes, provide:*

1. *The date the Authority to Operate (ATO) was granted: 2/27/2020*
2. *Whether it was a full ATO or ATO with Conditions: Full ATO*
3. *The amount of time the ATO was granted for: 3 year*
4. *The FIPS 199 classification of the system: 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.***

A new full ATO was granted on 2/27/2020. It's a 3 year ATO and a FIPS 199 MODERATE classification system.

## Section 9. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

| ID | Privacy Controls |
|---|---|
| **AP** | **Authority and Purpose** |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| **AR** | **Accountability, Audit, and Risk Management** |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-7 | Privacy-Enhanced System Design and Development |
| AR-8 | Accounting of Disclosures |
| **DI** | **Data Quality and Integrity** |
| DI-1 | Data Quality |
| DI-2 | Data Integrity and Data Integrity Board |
| **DM** | **Data Minimization and Retention** |
| DM-1 | Minimization of Personally Identifiable Information |
| DM-2 | Data Retention and Disposal |
| DM-3 | Minimization of PII Used in Testing, Training, and Research |
| **IP** | **Individual Participation and Redress** |
| IP-1 | Consent |
| IP-2 | Individual Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| **SE** | **Security** |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| **TR** | **Transparency** |
| TR-1 | Privacy Notice |
| TR-2 | System of Records Notices and Privacy Act Statements |
| TR-3 | Dissemination of Privacy Program Information |
| **UL** | **Use Limitation** |

| ID | Privacy Controls |
|---|---|
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

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

Quanisha L Jones 1394564 Digitally signed by Quanisha L Jones 1394564
Date: 2020.11.17 08:07:08 -05'00'

**Privacy Officer, Quanisha Jones**

Yolanda Maury 398226 Digitally signed by Yolanda Maury 398226
Date: 2020.11.05 11:58:42 -05'00'

**Information Security Systems Officer, Yolanda Maury**

Jennifer L. Treger 105837 Digitally signed by Jennifer L. Treger 105837
Date: 2020.11.05 11:44:30 -05'00'

**Information System Owner, Jennifer Treger**

## 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).

https://www.vba.va.gov/pubs/forms/VBA-21-526ez-ARE.pdf

https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf