Privacy Impact Assessment for the VA IT System called:

Resuscitation Quality Improvement-E (RQI 1Stop-E)

Veterans Health Administration (VHA)

VHA Office of Healthcare, Innovation and Learning

eMASS ID #1983

Date PIA submitted for review:

03/04/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Scott Miller	Scott.Miller@va.gov	717-413-1940
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	216-707-7726

Abstract

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

Resuscitation Quality Improvement-E (RQI 1Stop-E) is a collection of Training Licenses owned and operated by RQI 1Stop/Laerdal, is used by all VHA employees responding to a medical emergency. The RQI 1Stop portal hosts courseware for resuscitation training (American Heart Association Basic Life Support, Advanced Cardiac Life Support, Pediatric Advanced Life Support and Responder Layperson Training) that will help to track and improve resuscitation performance.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*
The system is. the (Resuscitation Quality Improvement) RQI 1Stop online platform. Simulation Learning, Evaluation, Assessment and Research Network (SimLEARN) Office within the VHA Office of Healthcare, Innovation and Learning is sponsoring the system and will own the data. However, the system itself is owned and operated by the SaaS Solution Vendor.

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
This software will support employment requirements laid out by VHA directives 1177, Cardiopulmonary Resuscitation, and 1101.05(2), Emergency Medicine. This system would be used by an estimated 250,000 employees annually to ultimately improve the delivery of care during a medical emergency. Cardiopulmonary Resuscitation (CPR) training is provided to Veterans Health Administration (VHA) employees through the VA Talent Management System (TMS) pointing to the (Resuscitation Quality Improvement) RQI 1Stop online platform. The system provides an option between an eCard certification or a quarterly e-Credential certification for a portfolio of resuscitation training to include Advanced Cardiac Life Support (ACLS), Basic Life Support (BLS), Pediatric Advanced Life Support (PALS) and Layperson (Responder) training. The electronic courseware is available in two modalities: The subscription modality, Resuscitation Quality Improvement (RQI), provides an online didactic training, followed by a hands-on skills session with a Voice-Assisted Manikin (VAM) to complete the skills competencies on a quarterly basis. The VAMS are located at the VA Medical Center (VAMC) or Community-Based Outpatient Clinic (CBOC). They are peripheral devices connected to a

designated laptop/desktop. Each VAM services approx. 250 employees. Contractors complete the training if it is worked into the contract language to participate in VA sponsored training. The license modality, HeartCode Complete, provides online didactic training followed by a hands-on skills session with a VAM every two years.

C. *Who is the owner or control of the IT system or project?*
Control of the system will be within VA, as outline in part A, while ownership and operation of the solution remain with the SaaS Solution Vendor.

2. Information Collection and Sharing

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*
This system would be used by an estimated 250,000 users annually to ultimately improve the delivery of care during a medical emergency. These users will include VA employees, contractors, volunteers, and clinical trainees.

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*
To track training and performance, the system primarily collects, processes, and retains the name, facility location, and TMS ID of VHA employees, contractors, volunteers, and clinical trainees.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*
Information sharing is between VHA and Talent Management System (TMS) SQL Server 1 and the RQI 1Stop system. The information shared is only that which is needed to provide courses to the end users and connect analysis of course uptake and course performance of end users to their profiles.

G. *Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*
The system is a SaaS system and will be operated in an AWS cloud environment, and will, therefore, not be operated on more than one physical site.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*
This software will support employment requirements laid out by VHA directives 1177, Cardiopulmonary Resuscitation, and 1101.05(2), Emergency Medicine. It is covered by SORN 76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802. https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*
The SORN needs to be amended due to age. This amendment has been requested. The system, and its use of cloud storage, is covered by SORN 76VA05 SYSTEM NAME:

Altered System of Records, General Personnel Records (Title 38)–VA. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802. https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf

4. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business processes.

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

Completion of this PIA will not require technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Business email, Facility location, TMS ID, Organizational affiliation, Job title, Department, Hire Date

PII Mapping of Components (Servers/Database)

RQI 1Stop consists of **1** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **RQI 1Stop** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Talent Management System (TMS) SQL Server 1	Yes	Yes	First, Middle Initial, Last Name, Email, Facility location, TMS ID, Organizational affiliation, Job title, Department, Hire date	To provide an on-line course to the end users in effective CPR, other healthcare related techniques & analytics.	1. Employee profiles are either directly sourced from HR system of record or manually entered through a web interface inside the VA

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

				Analysis of course uptake and course performance of end users	firewall. Data is communicated to TMS via Secure File Transfer Protocol and then stored in the encrypted data table that cannot be accessed via the application interface. 2. Least privilege principle is applied when granting administrative access to TMS where this data can be viewed in via the application interface. 3. Organization control

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

TMS supplies the identification and corresponding data for our VA employees taking these certifications. Non-VA employee user profile data is collected directly from the individual through the TMS self-enrollment module (which consists of an online web form: (https://va-hcm03.ns2cloud.com/learning/user/SelfRegistrationUserSelection.do).

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

TMS is the official system of record for compliance and completion. The User Profile must ultimately store the performance records for required trainings.

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

TMS must receive and store the pass/fail score of employees in resuscitation training completed through RQI 1Stop. The source of this score for TMS is RQI 1Stop.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The PII used for RQI 1Stop is pulled from an employee's TMS User Account. This information is then communicated to the RQI 1Stop portal for a user to access the program, conduct their training, and communicate their performance information back to their TMS User Account. User account data, which contains demographic information used to manage user training and development needs is collected through the following means: 1. TMS Self-Enrollment Module: Non-VA employees directly create a user account using the web form (https://va-hcm03.ns2cloud.com/learning/user/SelfRegistrationUserSelection.do) located on the TMS Homepage. 2. VA Payroll System: User accounts for VA employees are created through data feeds from the HR SMART system. 3. Education Data Repository (EDR): User accounts (both VA and Non-VA employees) are created and maintained through data feeds from the EDR. Nightly synchronization of user profile data between the EDR and TMS is supported by automated processes. 4. Direct TMS interface profile access: All TMS users can directly create and update certain data fields with their user account using the profile functionality with TMS interface. 5. Profile Maintenance: Provisioned TMS Administrators can create and manage TMS user accounts using the EDR web interface. The Profile Maintenance interconnection to TMS is a web services Application Program Interface (API) and enables real-time user profile creation and updates to provision administrators. RQI 2020 analytics is an inhouse analytics application integrated with RQI 1Stop platform (system) to provide customized analytics to the customer. These analytics are for the purpose of analyzing learner performance data to provide enhanced feedback and reporting to customers on learner progress and performance on the RQI 1Stop platform.

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

Information is not collected on a paper form.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Accuracy of the information in RQI 1Stop relies on the accuracy of the information in TMS with learner's organization or hospital, as they are obligated to provide correct & up to date information to create licenses in American Heart Association Resuscitation Portfolio. Routine daily automated processes are used as a quality control measure to maintain accurate and unique profiles in the TMS system so that VA may reliably deliver training compliance reports. Discrepancies are resolved through the data cleansing actions of TMS Administrators. TMS data accuracy is validated in four different ways: 1. TMS employee profile data is sourced from our HR system – currently HRsmart 2. Users are responsible for the accuracy of specific data elements for which there is no existing data source. 3. TMS administrators manage data of all sorts in the system in our decentralized model; and 4. Regular backend scripts and quality control audits that identify issues and, in some cases, resolve them automatically. Monthly data quality audits using elements of Lean Six Sigma (LSS) analysis began in June 2015 to measure and monitor the level of "accurate and unique" user profile records in TMS. The following data quality goals are the current focus areas for TMS audits: 1. Establish and maintain accurate user email addresses in the TMS system. 2. Establish unique user email addresses within TMS user profiles. 3. Establish unique Person IDs within TMS user profiles to eliminate duplicate profiles. 4. Establish accurate Org codes for TMS User Profiles. 5. Establish acceptable lifecycle times for profiles created in MSE and kept in self-domain. 6. Eliminate user profiles created in MSE and left in self-domain for VA employees. A series of data quality audits can provide measurable inputs to benchmark targeted process and data improvement areas. The data quality audit measurements will serve to prioritize issues and incrementally bridge the deficiency gaps by embedding quality assurance into processes to achieve an enhanced future state. In case of any changes to the learners' personal details, learners can send a service request to their organization admin to update such details in the system backend or directly they can send a request to RQI 1Stop customer services team.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

A commercial aggregator is not used.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802. https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section)

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Unnecessary personal information may be collected and shared.

Mitigation: Only required personal data is collected & processed in the RQI 1Stopsystem. RQI 1Stop program does not collect personal data from individuals. Specific Hospital or Institution shared their learner's data in Demographic file via SFTP server. It is the responsibility of hospitals or institutions to share the accurate, complete & up to date data with our RQI 1Stopsystem to create their learners' accounts & licenses.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use

Name	Analysis of course uptake and course performance by employees of Customer, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.	Analysis of course uptake and course performance by employees of Customer, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.
Personal Email Address	Analysis of course uptake and course performance by employees of Customer Communication about course progress and maintenance of competence, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.	Analysis of course uptake and course performance by employees of Customer Communication about course progress and maintenance of competence, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.
Business Email Address	Analysis of course uptake and course performance by employees of Customer Communication about course progress and maintenance of competence, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.	Analysis of course uptake and course performance by employees of Customer Communication about course progress and maintenance of competence, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.
TMS ID	Analysis of course uptake and course performance by employees of Customer, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.	Analysis of course uptake and course performance by employees of Customer, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.
Organizational Affiliation	Analysis of course uptake and course performance by employees of Customer, Separation of data from other Customers, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.	Analysis of course uptake and course performance by employees of Customer, Separation of data from other Customers, Access to courses by Customer employees, Access to course analysis and reports by Customer employees.
Facility Location	To create an Organization profile.	To create an Organization profile.
Department	Analysis of course performance on a department level for Customer.	Analysis of course performance on a department level for Customer.

Hire Date	Analysis of course uptake and course performance of employees of Customer, Evidence of course performance. Course Progress - Analysis of course uptake and course performance by employees of Customer, Evidence of course performance.	Analysis of course uptake and course performance of employees of Customer, Evidence of course performance. Course Progress - Analysis of course uptake and course performance by employees of Customer, Evidence of course performance.
Job Title	Analysis of course performance on a job title level for Customer.	Analysis of course performance on a job title level for Customer.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

RQI 2020 analytics (Internal System) is integrated with the system for the purpose of analyzing learner data to provide enhanced feedback and reporting to customers on learner progress and performance on the RQI 1Stop platform.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Analytics on progress and user performance will be added to User Profiles as part of the record of the completion their contractual obligation to complete these trainings. This performance is communicated in the form of a pass/fail grade needed to establish compliance or non-compliance of training. The reports are shared with leadership and CPR committees. Leadership for notification of non-compliance would be direct supervisor and/or executive leadership team to include Senior Nurse Executive and Chief of Staff. Both are responsible for the delivery of care provided at the facility. These analytics will also be used to inform decisions to improve trainings for better overall uptake and performance across the Administration.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Secure Socket Layer encryption connection (https), Protocol TLS 1.2 and Storage encryption – AWS Default encryption -Symmetric CMK encryption at rest (256 bit) are used to protect data in transit and at rest.

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

System does not collect nor process SSN.

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

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The PII used in the RQI 1Stop is mainly accessed via TMS. For this system, Administrators will have access to an employee's TMS profile.

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

The criteria, procedures, controls and responsibilities regarding access control are documented in the FedRAMP documentation for the system, the Customer Responsibility Matrix, and this PIA. The PII used in the RQI 1Stop is mainly accessed via TMS. For this system, Administrators will have access to an employee's TMS profile and will also have access to the reports produced in TMS that display the employee's performance in RQI 1Stop. This performance is communicated in the form of a pass/fail grade needed to establish compliance or non-compliance of training. The reports are shared with leadership and CPR committees. Leadership for notification of non-compliance would be direct supervisor and/or executive leadership team to include Senior Nurse Executive and Chief of Staff. Both are responsible for the delivery of care provided at the facility.
TMS management recently restricted the granting of the role that allows local administrators to create and assign responsibilities to lower-level administrators. This returns oversight control to the Department level. In addition to TMS Administrators taking role-based training for various levels of administration, all users are required to sign Rules of Behavior as part of their security awareness and privacy training. Administrator responsibilities are usually a collateral duty assigned by supervisors at the local level. Standardized TMS Administrator privileging rules need to be established and supported, as well as auditing logs and procedures put in place to ensure consistent implementation.

2.4c Does access require manager approval?

TMS management recently restricted the granting of the role that allows local administrators to create and assign responsibilities to lower-level administrators. This returns oversight control to the Department level. In addition to TMS Administrators taking role-based training for various levels of administration, all users are required to sign Rules of Behavior as part of their security awareness and privacy training.

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

Standardized TMS Administrator privileging rules need to be established and supported, as well as auditing logs and procedures put in place to ensure consistent implementation.

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

Safeguarding PII in TMS is a VA responsibility. RQI 1Stop is responsible for assuring safeguards of the information in transit and at rest within their system and when sharing to and from their system.

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*

First, Middle Initial, Last Name, Email, Facility location, TMS ID, Organizational affiliation, Job title, Department, Hire date are retained by the system.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The SORN states "b. Records in this system must be maintained and disposed of in accordance with General Records Schedule 1, and VA Records Control Schedule 10–1, the Office of Personnel Management Guide to Federal Recordkeeping, and the Memorandum of Understanding concerning this subject between VA, the Office of Personnel Management, and the National Archives and Records Administration". More specific to this system, VHA records office has proposed the use the following from Records Control Schedule 10-1: Retention Schedule 3015.3 - Occupational Health and Safety Training Records for training data elements, which includes Course completion, Course Progress, Course Performance Score, Date of Course Performance, Certificate of Competence; and Retention schedule 2201.2 - Intermediary Records has been proposed for all data elements going from TMS to the system, which includes Full Name, Email Address, Organizational Affiliation, Organization Address, Contact Number, Hire Date Job, Title, and Department. This calls for temporary retention with destruction upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. The final document or file would go to TMS when no longer retained by this system. Vendor requires retention of at least three years and VA Resuscitation Education, and Innovation Program requires 7 years retention.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes.

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

VHA records office has proposed the use of retention schedule 3015.3 - Occupational Health and Safety Training Records for training data elements and 2201.2 - Intermediary Records for all data elements going from TMS to the system.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Data will be destroyed in accordance with NIST SP 800-88, and VA Directive 6371. When required, electronic data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Digital media is shredded or sent out for destruction per NIST SP800- 88r1 as evidenced in the FedRAMP Audit reports. RQI 1Stop will follow NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process of any IT storage hardware used in the system. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

RQI 1Stop management & development team does not use personal data for new application testing or research purposes.

<u>3.6 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

<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: PII could become more vulnerable if retained by the system past verification of end of business need.

Mitigation: RQI 1Stop system collects only required information as part of the services. Appropriate record retention schedule will be followed once approved and data will be destroyed in accordance with VA Directive 6500, NIST SP 800-88, and VA Directive 6371 when no longer identified as needed for business use.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration (VHA)	Ensuring uniqueness of records in the application for data quality and reporting to accrediting bodies.	First, Middle Initial, Last Name, Email, Department	Shareable Content Object Reference Model package for exchange.
Talent Management System (TMS) SQL Server 1	Ensuring uniqueness of records in the application for data quality and reporting to accrediting bodies.	First, Middle Initial, Last Name, Email, Facility location, TMS ID, Organizational affiliation, Job title, Department, Hire date	Shareable Content Object Reference Model package for 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: An employee's personally identifiable information could be revealed to additional parties by internal sharing and disclosure.

Mitigation: Compliance/noncompliance associated with employees is patient safety related. Compliance status is shared with management (supervisors and executive leadership team) and is not shared to all hands. Monthly compliance reports are pulled by TMS admins or resuscitation program directors only.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
RQI 1Stop	Ensuring uniqueness of records in the application for data quality and reporting to accrediting bodies	First Name, Middle Initial, Last Name, Email, Facility location, TMS ID, Organizational affiliation, Job title, Department, Hire date	Contract Identifier 36C10X20G001 P00001	All data is encrypted in transit with transmission via TLS 1.2 Port: 443. REST API calls to the server must include a bearer token in the Authorization header.

SAP CDC (Customer Data Cloud)	User identity access details are transferred as part of the authentication	First Name, Last Name, Email	Title 38 Laerdal has signed the Data processing agreement with SAP CDC	All data is encrypted in transit with transmission via TLS 1.2 Port: 443. REST API calls to the server must include a bearer token in the Authorization header. By default, SAP Customer Data Cloud encrypts all personally identifiable information (PII) at rest using the AES-256 algorithm.

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> RQI 1Stop has integration with SAP CDC (External or third-party system) for user access authentication purposes and it shares limited personal data such as First name, Last name & email ID for authentication purposes. The user's activity & system logs are generated, reviewed & retained. This limited personal data could be compromised by being shared with external or third-party systems.

Mitigation: An access control procedure is implemented to ensure that only the right personnel will get access to the RQI 1Stopplatform. SAP CDC & Laerdal Medical have signed the Data Processing Agreement to protect the sharing of personal information on a legitimate basis.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The information shared is the same information that is already collected within TMS. The following VA System of Record Notices (SORNs) which are published in the Federal Register and available online applies to this system is 76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA. https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf. Current SORN List: https://www.oprm.va.gov/docs/SORN/Current_SORN_List_04182023.pdf. This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

A Privacy Act notice is provided on the web forms used to facilitate the TMS managed self-enrollment process and general profile maintenance (see Appendix A for a copy of this notice).

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Collecting information in TMS is considered the agency system of record per policy. The Privacy Act Notice adequately informs users of the Executive Order authorizing the data collection, the Purpose and Routine Use of their Data, and informs the user the furnishing of Data to TMS is voluntary, as well as the effects of choosing not to provide the data.

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

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

The training requirement is a condition of employment as well as a regulatory/licensure requirement. Collecting information in TMS is considered the agency system of record per policy. Therefore, individuals do not have the right or opportunity to decline to provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Information is used in accordance with the Privacy Act and is shared with VA employees when the information is needed in accordance with job requirements or when there is authority under b(1) of the Privacy Act. In addition, individuals may consent to additional uses of the information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 individuals may not receive notice that their information is being collected maintained, or disclosed by VA Learning University to RQI 1Stop prior to providing the information to VA.

Mitigation: Employees and contractors are on notice upon entering VA service that certain training may be required of them, and, as part of that training certain information may be required. It is important to note that the information provided is the same information already provided in TMS. The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1. Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Amendment procedures are specified in the SORN:C ONTESTING RECORD PROCEDURES: Current and former VA employees wishing to request amendment of their records should contact the Director, Department of Veterans Affairs Shared Service Center (00), 3401 SW 21st Street, Topeka, Kansas 66604. Individuals must furnish the following information for their records to be located and identified: Full name(s), date of birth, Social Security number, and signature. To facilitate identification of records, former employees must also provide the name of their last Department of Veterans Affairs facility and approximate dates of employment.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt.

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

This is a Privacy Act system.

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.*

Accuracy of personal information lies with learner's organization or hospitals, as they are obligated to provide correct & up to date information to create licenses in RQI 1Stop system. In case of any changes to the learners' personal details, learners can send a service request to their organization admin to update such details in the system backend or directly they can send a request to RQI 1Stop customer services team. Amendment procedures are specified in the SORN: CONTESTING RECORD PROCEDURES: Current and former VA employees wishing to request amendment of their records should contact the Director, Department of Veterans Affairs Shared Service Center (00), 3401 SW 21st Street, Topeka, Kansas 66604. Individuals must furnish the following information for their records to be located and identified: Full name(s), date of birth, Social Security number, and signature. To facilitate identification of records, former employees must also provide the name of their last Department of Veterans Affairs facility and approximate dates of employment.

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.

In case of any changes to the learners' personal details, learners can send a service request to their organization admin to update such details in the system backend or directly they can send a request to RQI 1Stop customer services team. It is specified in the SORN as stated above.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Learners have access to their profile to verify the accuracy of their information and make the necessary corrections or updates. In case of any additional access needed for updates, the request will be verified and provisioned considering the applicable privacy laws & the data access rights. Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3 In addition to the formal procedures discussed in question 7.2.

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. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
<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> Inappropriate parties could gain access to an employee's performance record and personally identifiable information.

<u>Mitigation:</u> Access control procedure has been implemented to enforce approved authorizations for logical access to information and system are provisioned.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Access control procedure has been implemented to enforce approved authorizations for logical access to information and system. Access is established in TMS based on several criteria outlined in 8.1c.

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

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

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

The different roles that have been created are as follows: Cloud Level 1 Engineer, Cloud Level 2 Engineer, Sr. Cloud Level 2 Engineer, Cloud L3 Engineer, App Support Team – L1, App Support Team – L2, App Support Team – L3, App Support Team – Lead, DB admin, Implementor. Enterprise admin, Unit admin, Institute Admin, and Learners. Their access is further broken down by whether they are internal (VA) or external (RQI/Laerdal). Access is further identified by Logical Access level, which can be categorized as: Privileged, Non-Privileged, or No Logical Access. The Sensitivity Level or data accessed per role is also categorized by: Limited, Moderate, Severe, and High-Risk. Authorized privileges are assigned per and break down to the following: Pseudo administrative access, Full administrative access (root), Read & Write access (UI), Read & Write access, Enterprise Admin, Unit admin/department admin, and Institute admin. Functions performed vary and are specific to the role assigned.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

No, contractors do not have access to PII in the system.VA clinical contractors only participate in the training and only have access to their individual assignments. As such, no contractor confidentiality agreement has been developed.

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.

General Data Protection Regulation (GDPR) specific training & awareness has been provided to the resources supporting & managing the RQI 1Stop system. Additional training is required by VA employees and associated clinical staff (WOC, Contractors, Trainees) who are all required to complete the annual Information Security and Privacy training within TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>

5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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

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

VA Sponsored FedRAMP ATO process is the initial A&A process for the RQI 1Stop SaaS application and is In Process. The following items are included in this process: Security Plan, Authorization, and Risk Review. The estimated IOC date is 06/24/2024. The system is currently classified as Low Impact.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The system does use cloud technology through AWS and the vendor is currently seeking FedRAMP and agency authorization through the Product Engineering Team within the Data Transformation Center. RQI 1Stop is a Software as a Service (SaaS).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

There is no contractual agreement between the VA and the CSP. The agreement is between the VA and the SaaS solution vendor RQI1Stop. However, the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is 36C10X20G001 P00001.

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

AWS does collect data on the VMs and containers it supplies to its customers. They do not access application/system specific logs. Data generated within the cloud environment is protected and controlled by customer (or Laerdal) with encryption at rest AES 256, customer managed key. Security and Compliance is a shared responsibility between AWS and the Customer (or Laerdal or RQI program).AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customer (or Laerdal) responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customer (or Laerdal) is responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The selected CSP inherits the following controls from FedRAMP- Authorized Cloud Infrastructure Provider (Amazon Web Services) that includes: Physical and Environmental controls, Patch Management (on infrastructure level), Configuration Management (on infrastructure level), Awareness & Training (on infrastructure level)Service Provider (Amazon Web Services) claims responsibility for protecting the hardware, infrastructure software, networking, and facilities that run AWS Cloud services.

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

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

System does not utilize Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.04.01 11:40:32 -04'00'

Privacy Officer, Nancy Katz-Johnson

SCOTT MILLER

Digitally signed by SCOTT MILLER
Date: 2024.04.01 11:51:47 -04'00'

Information System Security Officer, Scott Miller

AIMEE BARTON

Digitally signed by AIMEE BARTON
Date: 2024.04.01 16:11:35 -04'00'

Information System Owner, Aimee Barton

APPENDIX A-6.1

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

https://www.govinfo.gov/content/pkg/FR-2000-07-20/pdf/00-18287.pdf

https://www.oprm.va.gov/docs/SORN/Current_SORN_List_04182023.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices