Privacy Impact Assessment for the VA IT System called:

Issio Workforce Optimization Platform

Veteran Affairs Palo Alto Health Care System (VAPAHCS)

Veterans Health Administration (VHA)

Date PIA submitted for review:

6/13/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	kamilah.jackson@va.gov	513-288-6988
Information System Security Officer (ISSO)	Danny O'Dell	danny.odell@va.gov vharicisosupport@va.gov	(650) 43-5000 ext 63844
Information System Owner	Rob Maas	rob.maas@va.gov	(352) 672-3028

Abstract

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

Issio's Workforce Optimization Platform functionality will help leadership ensure preparedness and resilience to provide continual service in a time of crisis. In a crisis, Issio allows leaders to make time-sensitive labor work-force decisions that can be quickly deployed via skill set search and the float pool. System is a SaaS cloud-based solution that will utilize AWS infrastructure to host va.issio.net.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Issio Workforce Optimization platform is owned by the Veteran Affairs Palo Alto Health Care System (VAPAHCS). Veteran Affairs Palo Alto Health Care System (VAPAHCS) is looking to expand the capabilities of the current Issio Workforce Optimization Scheduling and Float pool solution. The existing ATO authorized limited data collection and operated as a pure SaaS product without integrating with any VA systems. VAPAHCS now has plans to expand the Issio features to include predictive analytics that will help leadership manage Nursing Hours Per Patient Day (NHPPD) metrics and meet Veterans Integrated Services Network (VISN) Goals. To do so, the Issio application would require VA census and bed data be entered into the application to determine proper NHPPD goals and staffing needs accurately. At this time, the data is being entered manually by nurses which is time consuming and cannot always be entered frequently. The updated project scope would allow for an automated extract, transform, load (ETL) process to pull census data from our VA's Corporate Data Warehouse (CDW) and send it to an Issio database daily.

Issio's Workforce Optimization Platform functionality will help leadership ensure preparedness and resilience to provide continual service in a time of crisis. It is estimated 2,500 users will use this system. In a crisis, Issio allows leaders to make time-sensitive labor work-force decisions that can be quickly deployed via skill set search and the float pool. System is a SaaS cloud-based solution that will utilize Amazon Web Services (AWS) infrastructure to host va.issio.net. This system is currently FedRAMP authorized at Low impact, not Moderate. The Cloud Service Provided (CSP) is willing to move forward with FedRAMP authorization at Moderate and is working with VA's Project Special Forces SaaS Team. The system is being assessed through VA ATO process and will be reviewed by ISSO, Case Manager, Risk Review, Authorizing Official (AO) Designated Representative, and AO.

The system will contain data elements including time, VA census, bed data, department, role, PTO details, and daily schedule details. A Data Security Categorization (DSC) has been completed and the data rated at Moderate impact. The magnitude of harm would be Moderate impact.

The sources of information used to populate the application are currently being maintained by established responsibly parties. The systems required to attain the needed information are as follows: Corporate Data Warehouse (CDW), Bed Management Solution (BMS), HRSmart, Priv Plus, and Vet Pro. The Corporate Data Warehouse (CDW) is the VHA longitudinal database that consolidates VHA data from many sources, such as VistA and other national databases. CDW will only be used to collect patient census data for the facility. The Bed Management Solution (BMS) contains patient bed information, such as number of operating beds in a specific ward or facility. HRSmart is a system of records maintain by Office of Human Resources (OHR). Priv Plus is a credentialing system for both Nursing and Physician Staff privileged through the Medical Staff Coordinators under the Chief of Staff. Vet Pro is another credentialing system primarily used for Registered Nurses (RN's) who are privileged through the Nurse Recruitment Office. All PII information is maintained by the respective services and server as the responsible parties to ensure accuracy and consistency of all data provided.

The anticipation is that other VA facilities will use this in the future and the number of users will grow, but currently only in use at Palo Alto Health Care System. The PIA will not lead to changes to business processes or technology

Existing SORNs: CDW - Patient health record detailed information, including information from:

Patient Health Record—VA SORN 24VA10A7
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Patient National Databases—VA SORN 121VA10A7. BMS –
https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA SORN 79VA10.
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

HR Smart – VA SORN 171VA056A – managed through the Human Resources Information Systems Shared Service Center (HRIS SSC).
https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

Priv Plus & Vet Pro - Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E.
https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf

Legal citations: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E.

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.

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

☐ Gender
☐ Integration Control Number (ICN)
☐Military History/Service Connection

☐ Next of Kin
☒ Other Unique Identifying Information (list below)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>
VA census (Admission Date, Sta3n, Ward, RoomBed, BedOccupiedDayPrior (binary) (calculated field), BedDaysOfCare (continuous) (calculated field based on prior day LOS)), bed data, VA employee name, VA employee email address, VA employee phone number
Variable Data Entry Fields: Long term schedule (Working dates, Start time, Department, Role, Days off, Reason for day off, PTO or not) Daily Schedule (Start time, End time, Facility, Department, Messages)

PII Mapping of Components

Issio Workforce Optimization Platform consists of **two** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Issio Workforce Optimization Platform** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/ No)**	**Does this system store PII? (Yes/ No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
SQL Server 1	Yes	Yes	Required Information: • VA employee name • VA employee email address • VA employee phone number (personal or work cell phone) • Employee credential certification VARIABLE DATA ENTRY FIELDS:	• Staff Scheduling • Communicating schedule assignments and changes, multi-factor authentication • Tracking certification validity	Issio has FedRAMP Low authorization. VA Enterprise Security Architecture Cloud Security is working with the vendor team on a System Security Plan aligned with FedRAMP

			• Long Term Schedule ○ Working dates ○ Start time ○ Department, Role ○ Days off ○ Reason for day off (VATAS Preset Options) ○ Annual Leave (AL) or not • DAILY SCHEDULE: ○ Start time ○ End time, ○ Facility ○ Department ○ Messages		moderate requirements.
Corporate Data Warehouse (CDW) Fact tables: • CDWWork.Inpat.Inpatient Dimension tables (Non-PHI): • CDWWork.Dim.Location • CDWWork.Dim.RoomBed	Yes	Yes	• Admission Date • Sta3n • Ward • RoomBed • BedOccupiedDayPrior (binary) (calculated field) • BedDaysOfCare (continuous) (calculated field based on prior day LOS)	To calculate hospital census and operating beds for predictive analysis to determine accurate staff to patient ratios.	Issio has FedRAMP Low authorization. VA Enterprise Security Architecture Cloud Security is working with the vendor team on a System Security Plan aligned with FedRAMP moderate requirements.

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 systems required to attain the needed PII are as follows: HRSmart, Priv Plus, Vet Pro, Bed Management Solution (BMS) and the Corporate Data Warehouse (CDW).

HRSmart is a system of records maintained by OHR (Office of Human Resources). HR Smart will be used to pull employee name, Email address and phone number data.

Priv Plus is a credentialing system for both Nursing and Physician Staff privileged through the Medical Staff Coordinators under the Chief of Staff. Priv Plus will be used to provide up to date credentials for physicians and Nurses.

Vet Pro is another credentialing system primarily used for RN's (Registered Nurses) who are privileged through the Nurse Recruitment Office. Vet pro will also be used to provide up to date credentials for nursing staff.

Bed Management Solution (BMS) will be used for patient bed information, such as number of available operating beds in a specific ward or facility. Data will contribute to predictive analytics functionality.

The **Corporate Data Warehouse (CDW)** aggregates all Electronic Health Record Data into a large database. We will collect specific data related to patient census and operating bed availability to determine appropriate staff to patient ratios for each ward using predictive analytics.

All PII info in maintained by the respective services and server as the responsible parties to ensure accuracy and consistency of all data provided.

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.

HRsmart is a system of records maintained by OHR (Office of Human Resources). HR Smart will be used to pull employee name, Email address and phone number data. Employee Information is currently being collected manually by service management and stored on the Issio Cloud Platform.

Priv Plus is a credentialing system for both Nursing and Physician Staff privileged through the Medical Staff Coordinators under the Chief of Staff. Priv Plus will be used to provide up to date credentials for physicians and Nurses. Medical Staff Coordinators, including credentialing and privileging managers, maintain the Priv Plus system. Credential information is manually collected from Priv Plus by VA Management Staff and entered into the Issio application.

Vet Pro is another credentialing system primarily used for RN's (Registered Nurses) who are privileged through the Nurse Recruitment Office. Vet pro will also be used to provide up to date credentials for nursing staff. Medical Staff Coordinators, including credentialing and privileging managers, maintain the Vet Pro system. Credential information is manually collected from Vet Pro by VA Management Staff and entered into the Issio application.

Bed Management Solution (BMS) will be used for patient bed information, such as number of available operating beds in a specific ward or facility. Census and Operating Bed data will eventually be set up to automatically pull data from CDW using an Extract Transform Load (ETL) process. The process will run a SQL query to collect the said data and export it to a Comma Separated Value (csv) format, then uploaded into the Issio Cloud Platform.

The Corporate Data Warehouse (CDW) aggregates all Electronic Health Record Data into a large database. We will collect specific data, using a custom SQL query, related to patient census and operating bed availability to determine appropriate staff to patient ratios for each ward using predictive analytics. Eventually we will be set up to automatically pull data from CDW using an Extract Transform Load (ETL) process. The process will run a SQL query to collect the said data and export it to a Comma Separated Value (csv) format, then uploaded into the Issio Cloud Platform.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The system continually checks the database for accuracy and validity of the information as per FedRAMP Low SSP moving to FedRAMP Moderate certification within the next year. Attempts to enter non-numeric characters into phone number fields are rejected (the field simply does not populate with the characters being typed unless those characters are numbers). Likewise, attempts to enter an email in an invalid email format are rejected, and this is indicated by a red highlight that disappears when correct email address format is used. As well, both first and last name fields are required to be filled before a user profile can be saved.

Currently there is no interface with any system within any other Federal Agency for confirming for accuracy and consistency with internal federal system - for example HR systems. As it stands now, the VA Issio user (Manager, Administrator) would have to check the information manually - for example confirm that a license listed as expired in Issio is in fact expired (potentially the new expiration date has been updated in another system but not in Issio). Issio has built interfaces with a number of different information systems, this is something we specialize in and configuring an interface with an HR system for example would be within our capabilities. Interface construction is driven by customer demands and requests.

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

38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: . There is a risk employee names, certification types with expiration dates and personal telephone numbers could be accessed by unauthorized individuals. Census data and operational bed status do not pose any privacy risk if exposed, due to not being associated with any PHI or PII. Census data strictly represents the number of used or available operating beds in the healthcare system.

Mitigation: Only the minimum amount of information is requested from the HR Smart, C&P systems and the Corporate Data Warehouse (CDW) and only authorized individuals have access to the database.

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.

- **Employee name:** Required for scheduling purposes.
- **Employee/personal phone number:** Required for communication purposes and to inform the employee of scheduling changes.
- **Employee Email:** Required for communication purposes and to inform the employee of scheduling changes.
- **Employee Credentials:** Required to ensure current and valid certifications are in place.
- **BMS operating bed availability per ward and facility level:** Required for predictive analysis to determine accurate staff to patient ratios.

- **CDW Census and Operating beds data:** Required for predictive analysis to determine accurate staff to patient ratios.
    - **Admission Date:** Required to determine length of stay (LOS) for a patient.
    - **Sta3n:** Required to confirm what health care system data represents.
    - **Ward:** Required to determine staff patient ratio by ward.
    - **RoomBed:** Required to confirm which beds are in use or available.
    - **BedOccupiedDayPrior(binary) (calculatedfield):** Required to determine the length of stay (LOS) for a patient.
    - **BedDaysOfCare (continuous) (calculated field based on prior day LOS):** Required to determine the length of stay (LOS) for a patient.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The only tools available to analyze the data would be the built-in report functionality, called "Labor Analytics" in the Issio cloud platform. The most relevant and important individual tools contained within Labor Analytics are "NHPPD Analysis", which as the name suggests, provides a collated view of NHPPD information which is drawn from each individual facility (those that track NHPPD) using staffing info and patient census info. The reporting and analytics functions could be leveraged to quickly identify workload and balance. Many employees have a cap on the number of hours that can be worked in each pay period and the report will help provide management insight on an employee's scheduled time. More advanced predictive analytics that incorporates patient census and operating bed data, would also reveal patient-to-staff ratios. These reports can inform management what wards are understaffed or overstaffed on an hourly and daily basis. Currently, this information is already being tracked in a more manual process and reporting functions would help automate the process.

There is also "Benchmarks" which aggregates staff data into a chart view. For example, a manager can see using Benchmarks how many hours of time off each staff member in their unit has taken, or they can see a breakdown of how many days they have met their NHPPD target. Finally, “Briefing Reports” gather data from a unit or service line of units to provide managers and admins with a daily/weekly report that, like above, contains info on NHPPD, time off, who is working where, etc. A summary of what is going on in a unit or service line on a given day or in a given week.

Finally, there is also the “Patient Capacity Whiteboard”, which pulls staff schedule and patient census info from each unit to provide a single pane view of how each unit is doing in terms of over vs. understaffing.

In short, all of these tools aggregate various types of staffing and schedule data together to provide useful insights for managers and administrators, but the tools do not produce novel information about individuals as such.

2.3 How is the information in the system secured?

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

All data is encrypted in transit and at rest using industry standards. Where available, we use only encryption methods that meet NIST FIPS 140-2 standards. Everything that Issio itself codes is to the FIPS standards, and where AWS has an option to limit things to FIPS 140-2, we have implemented that option. Of course, Issio cannot control everything on the public internet, but we do insist on the best encryption available to us. eg: we do not support TLS 1.0 or 1.1, but we require 1.2 and support 1.3.

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

Issio does not store Social Security Numbers and has no plans to do so in the future.

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

As above, data including PII/PHI is encrypted in transit and at rest in the Issio Information System and likewise in the additional FedRAMP-authorized Moderate and High information’s that Issio uses in support. Security risks and vulnerabilities are tracked and amended as they appear per Issio's Continuous Monitoring Plan and testing obligations, and relevant security alerts and updates (such as those provided by CISA) are communicated as appropriate to Issio staff.

All Issio employees and contractors sign and comply with a Rules of Behavior agreement that stipulates steps to be taken to ensure information security, and likewise sign and agree to a password protection agreement to ensure account security. All employees and contractors undergo annual foundational security awareness training, as well as role-specific training for higher sensitivity positions and security incident and contingency training. All access to production data - among the limited number of employees who do have access - is apportioned according to the principle of least privilege, and access privileges are monitored by Issio security staff on an ongoing basis.

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

2.4 <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. <u>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.</u>

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

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

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

Add answer here:

Access to PII will primarily be provided to management staff in charge of scheduling. If unable to attain information from HRSmart, employees will provide their name, email and\or telephone number to the department for scheduling. The information will be stored on Issio Cloud Platform and will be removed if the employee separates from the facility. Issio has security measures in place to safeguard the employee's personal information. Issio has completed an SSP based on FedRAMP Low requirements and that has been reviewed by VA's ESA CS team. Issio is moving forward with FedRAMP Moderate certification within the year.

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 system collects and retains the following information for the time period where the customer is using the product:
Staff names, cell phone numbers, certification names and date of expiration, patient census and operating beds data (Admission Date, Sta3n, Ward, RoomBed, BedOccupiedDayPrior, BedDaysOfCare). The information is securely housed in the Issio Information System under ESA CS reviewed SSP Low. FedRAMP moderate certification is currently being pursued.

3.2 How long is information retained?

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The information is kept in the system until:
1. The staff member is no longer employed by the customer (the staff member's information would be deleted from the system by the VA Issio User)
2. The customer is no longer a customer (the account would be erased with all the information within it deleted)- a flat file of all data could be transmitted to former customer.

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.

NARA – Page 63, RCS 10-1 (**N1-015-10-07, item 1**)

Item Number: 1150.1

Records Description:

Health Care Provider Credentialing and Privileging Records.

Information pertaining to the individual's name, address, date of birth, social security number, name of medical or professional school attended and year of graduation. It also includes information involving the individual's license, registration or certification by a state licensing board and/or national certifying body, citizenship, honor and awards, professional performance, experience, judgement, education qualifications, Drug Enforcement administration certification, information about mental and physical status evaluation of clinical and/or technical skills, and involvement in any administrative, professional or judicial proceedings.

a. Paper Source Documents. Hardcopy version of information manually entered or scanned into electronic credentialing and privileging records.

1. Paper records that have not been scanned into electronic system.

2. Paper records that have been scanned and verified for accuracy into an electronic system.

b. Electronic Files. Electronic version of information entered directly into the electronic credentialing and privileging records information system.

Disposition Instructions

Temporary. Cutoff 3 years after employee separates from VA employment; transfer to offsite inactive storage. Destroy by WITNESS DISPOSAL 30 years after employee separation from VA employment.

Temporary. Destroy by WITNESS DISPOSAL after verification for accuracy.

Temporary. Delete 30 years after the last episode of employment, appointment, contract, etc. from VA.

Disposition Authority:

N1-015-10-07, item 1

VHA Records Control Schedule 10-1 https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

VA Records management procedures are addressed in VA Handbook 6300.1
https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=475&FType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are disposed of in accordance with VA Directive 6500.
https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=932&FType=2 and OIT-OIS SOP MP-6-Electronic Media Sanitization procedures.

The information in the system is destroyed by:

1. Individual user accounts (e.g., staff users) can be deleted by a customer user with higher access privilege (e.g., a manager user type) if that subordinate user is no longer employed by the customer or needs to be removed from the system account in which that user exists for another reason. This is done in the “Staff” section of the application by selecting the employee’s name and clicking the “Delete” button. If an individual user is deleted, Issio retains that user’s information for customer use - for example, if a user were to be deleted accidentally or if that staff member needed to have their profile migrated to another customer facility account - but it is otherwise invisible and inaccessible. Likewise, individual facility accounts (e.g., an environment corresponding to an ER) can be deleted, including the customer users associated with that facility account, at customer request. Like users, these deleted accounts are retained in case they need to be reinstated or for other customer uses but are inaccessible and frozen. The steps to remove such individual are as follows: Go to Staff section > Select employee > Delete Employee

2. If a customer terminates or concludes their contract with Issio, that customer’s system facility accounts (of which a customer might have multiple) will be deleted in their entirety, including all associated users. The account termination process is conducted by Issio’s DevOps and Security Teams. The process mainly involves the deconstruction of the relevant IaaS AWS infrastructure supporting that customer account and elimination of customer information from Issio’s production database, which contains both customer-specific facility account configurations and user information. If the customer requires the system facility account information that is to be deleted, including all associated user information, Issio can provide that information as a flat file. All related information held by Issio, for example system facility account configuration spreadsheets that customers initially provide so that Issio can configure customer accounts, are likewise eliminated in their entirety or re-provisioned back to the customer if requested. This is likewise the responsibility of Issio’s Security Team. Issio otherwise retains no physical customer information.

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

The system uses multiple techniques and features to minimize the risk to individuals' PII. The Issio Information System uses stringent data security and protection methods, processes, and policies to conform to ESA CS SSP Low ATO process. In addition, the Issio Information System is structured in a need-to-know access control environment, where only those individuals with a "need to know" have access to the information they need to complete their work.

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?

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> There is a risk with sharing personnel information with CSP. The phone number, credentials, and email are associated with a personnel profile. There is a risk with sharing patient census and operating bed data with CSP. Patient census and operating bed data includes the following data points: Admission Date, Sta3n, Ward, RoomBed, BedOccupiedDayPrior, BedDaysOfCare.

Mitigation: This information is deleted as soon as employee no longer works for VA or VA no longer uses Issio as a CSP. The retention is based on NARA 1150.1. This information is deleted as soon as VA no longer uses Issio as a CSP.

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***
N/A	N/A	N/A	N/A

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***

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: N/A

Mitigation: N/A

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***
N/A	N/A	N/A	N/A	N/A

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: N/A

Mitigation: N/A

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 VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

Notice is also provided in the following SORN's:
Human Resources Information Systems Shared Service Center 171VA056A

Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E.
Patient Health Record—VA SOR 24VA10A7
Patient National Databases—VA SOR 121VA10A7
Veterans Health Information Systems and Technology Architecture (VistA) Records-VA SOR 79VA10
HR Smart – Human Resources Information Systems Shared Service Center (HRIS SSC) 171VA056A
Priv Plus & Vet Pro - Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E

No written notice is provided specifically for the use of Issio. Employees are notified verbally by their service managers when entered into the Issio System.

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

Staff members can decline to submit their personal cell phone numbers. In this case, they will automatically be notified of their schedule and messages by email and/or calendar sync.
This method is not as immediate as the cell phone, but some of our commercial clients prefer the email notification method. If the employee did not provide either personal cell phone or email or any other contact, then they would not be able to perform their duties during their scheduled shift.

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

If Issio retains their cell phone number and they decide to use email for notifications, the user can set their own preference.

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.

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

<u>Principle of Transparency:</u> 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 no written notice associated with sharing information to Issio CSP. Information shared with CSP, potentially could be exposed to unauthorized individuals without their awareness.

Mitigation: The individual can choose to not share their personal cell phone number in Issio. The individual is provided notice when sharing their information through VA SORN's:

HR SMART-Human Resources Information Systems Shared Service Center - 171VA056A
Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E.
Patient Health Record—VA SOR 24VA10A7
Patient National Databases—VA SOR 121VA10A7
BMS - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA SOR 79VA10
HR Smart – Human Resources Information Systems Shared Service Center (HRIS SSC) 171VA056A
Priv Plus & Vet Pro - Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E

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.

Operations, Admin and manager user types are given temporary login IDs and passwords (given these over the phone or in person). They login to the Information system and are forced to do multi-factor authentication and then change their passwords.

Staff get an initial SMS (Short Message Service) and from that they can access their information (only theirs). Only authorized individuals are permitted access to Issio. The only information contained within Issio is the employee’s name, email, telephone number and certifications. The information is available among employees and therefore already have access to the information.

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.

Individuals can change their own name and contact information through their own mobile device via clicking a link in the SMS message they can edit their own information - they only have access to their information - no one else's info. The system manager will be responsible for updating and correcting inaccurate or erroneous information.

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.

Initial SMS messages to the staff explain how they edit their own information through the SMS message and link that opens a browser on their mobile device.
Employees are informed at the time of hire of the process for correcting personal information collected into the VHA System of Records by contacting the Human Resources Department.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

The individual can contact their manager/administrator, or they can contact Issio customer support.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is risk sharing PII with CSP. PII provided could potentially be incorrect, leading to employees not receiving notification. Redress is in the control of the employee, although the employee may not understand how to fix their won data. Supervisors who enter information manually could potentially mix up PII and expose their name, email or phone number to another employee.

Mitigation: The individual can update their own information if there are any errors. An individual does not have access to anyone's information except their own. The initial sign up provides information on how to correct information errors, there is also a help desk through the CSP.

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.

Access control in the Issio Security System is clearly controlled and defined, however, the customer has the ultimate responsibility to assign their staff to the correct user roles with the minimum required functionality and access. User types are described below, and Issio Customer Support can help customers determine which role is appropriate for the different employee types.

Non- Privileged User Types: (customer) Operations User Type - Customer user. Oversees multiple facilities - typically a VP of operations or Sr. Level Administrator with purview over multiple facilities. Responsible for operations and/or financial success of multiple facilities. this user type typically is interested in reports and analysis

Admin User Type - Single site administrator/ director - Responsible for operations and/or financial success of single facility. This user type typically is interested in reports and analysis. Only has access to data from one facility.

Manager User Type - Staff scheduling manager overseeing multiple staff typically in one department at one facility. Interested in staff scheduling functionality, minor reports, communications

Staff User type - extremely limited access to their own schedule information, name, phone number, email address, notification preferences and skill sets. This data is accessed through SMS and unique token link specific for their individual phone and their individual message. Staff user type does not have login privileges to the application.

Issio establishes a point of contact with the VA Medical Center who has the authority to add and remove members.

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.

Issio will have access to employee name, emails, and telephone numbers that are listed. Access would only be required for support services. NDA is part of VA on boarding.

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.

All VA employees are required to complete yearly VA10176 Information Security and Rules of Behavior training. Individuals who have access to protected health information are also required to take the VHA Privacy and HIPAA Focused training VA10203.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*

4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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.***

1. The Security Plan Status, - In process
2. The Security Plan Status Date, - In process
3. The Authorization Status, - In process
4. The Authorization Date, - In process
5. The Authorization Termination Date, - In process
6. The Risk Review Completion Date, - In process
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH). – Moderate

Initial Operating Capability (IOC) Date: Project January 2023

Section 9 – Technology Usage

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

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

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

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

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

This Information System utilizes Amazon Web Services (AWS) infrastructure to host va.issio.net. This is a commercial instance of AWS and does ***not*** reside inside the VA Enterprise Cloud (VAEC). The AWS instance does have FedRAMP Low Authorization, and it is currently in process of pursuing a VA Sponsored FedRAMP Moderate Authorization.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

Current contract in place (NNG15SD29B) has SaaS language included, outlining FedRAMP requirements and PHI data ownership.

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.

Issio is required to record and store logs of all user activity, as well as to keep audit logs of cloud services at AWS. These data are Issio's but can be provided to the VA if and as needed.

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.

Contract included FedRAMP Authorized SaaS language that outlines CSP responsibilities to comply with FedRAMP Authorization and Agency ATO requirements. These approvals layout the security responsibilities roles for the CSP in order to allow VA data to be stored within their environment. All CSP employees and contractors sign and comply with a Rules of Behavior agreement.

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

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

N/A

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
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.

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.07.27 14:55:16 -04'00'

Privacy Officer, Kamilah Jackson

DANNY M O'DELL 203007

Digitally signed by DANNY M O'DELL 203007
Date: 2022.07.28 09:02:05 -07'00'

Information Systems Security Officer, Danny O'Dell

Robert J. Maas 516033

Digitally signed by Robert J. Maas 516033
Date: 2022.07.28 12:52:31 -04'00'

Information Systems Owner, Rob Maas

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).

Human Resources Information Systems Shared Service Center – SOR 171VA056A

https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf

Health Care Provider Credentialing and Privileging Records- SOR 77VA10E2E

https://www.federalregister.gov/documents/2020/02/07/2020-02477/privacy-act-of-1974-system-of-records

https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf