Privacy Impact Assessment for the VA IT System called:

AcuStaf Software Assessing

Office of Nursing Informatics

Veterans Health Administration

Date PIA submitted for review:

August 23, 2023

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)	Thomas Orler	thomas.orler@va.gov	906-221-9990
Information System Owner	Sheila A. Ochylski	sheila.ochylski@va.gov	202-461-5881

Abstract

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

AcuStaf Labor Management System is a resource management system used by VHA staff at various VA locations to schedule nurses and other employees, collect data related to staffing and generate reports.

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. The IT system name and the name of the program office that owns the IT system.

AcuStaf Software – Office of Nursing Informatics

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

AcuStaf Software is a workforce management technology that provides automated staffing, scheduling and labor management functionality. The application is web-based and provides the ability to create, view and edit staff schedules, and generate management tracking and variance reports. The staffing and scheduling functionality includes time and attendance automation, as well as personnel scheduling. AcuStaf allows definition of employee positions, skill levels and credentials, and required hours. Categories for time and attendance hours include compensatory time, overtime, regular time, holiday, sick and vacation time. The reporting function includes more than 200 standard reports and ad-hoc reporting is available at the data element level. The labor management functionality currently integrates with existing human resource and payroll systems.

C. Indicate the ownership or control of the IT system or project.

AcuStaf Software is a privately deployed managed service maintained by the vendor

2. Information Collection and Sharing

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

Over 100,000 records

E. A general description of the information in the IT system and the purpose for collecting this information.

AcuStaf Software is used to advance the VA workforce process management for its improved patient care through VHA directive 1351 compliance. AcuStaf Software is a workforce management technology that provides automated staffing, scheduling and labor management functionality. The application is web-based and provides the ability to create, view and edit staff schedules, track staff licenses and credentials, and generate management tracking and variance reports. The staffing and scheduling functionality includes time and attendance automation, as well as personnel scheduling. AcuStaf allows definition of employee positions, skill levels and credentials, and required hours. Categories for time and attendance hours include compensatory time, overtime, regular time, holiday, sick and vacation time. The reporting function includes more than 200 standard reports and ad-hoc reporting is available at the data element level. The labor management functionality currently integrates with existing human resource and payroll systems. Employee data is needed for identification and work information to best schedule them. Patient SSNs can be used as the unique identifier for HL7 Data received from the VA VistA ADT interface if the Patient ID is not provided. Patient information is collected for the use of nursing assignments to ensure equitable workload. Workload and employee information is used to automate these staffing decisions.

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

AcuStaf Software does not share any data outside of the VA

G. 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.

Each facility is provided a privately deployed server. These underlying server and software configurations are controlled by templates and configuration policies to ensure consistency in the maintenance and protection of PII.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

PII is collected by the VA Office of Nursing Informatics.

The applicable SORN is 79VA10, Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

Patient SSNs can be used as the unique identifier for HL7 Data received from the VA VistA ADT interface if the Patient ID is not provided. Patient information is collected for the use of nursing assignments to ensure equitable workload. Workload and employee information is used to automate VHA Directive 2010-034 and VHA Directive 1750. Executive Order 9397 gives authority to collect SSN and the authority for maintaining the information is Title 38 USC section 7301(a) which is in the VistA SORN 79VA10P2.

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 current SORN does not require any type of update – it currently covers cloud usage and storage.

D. System Changes

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

No changes will be required

K. *Whether the completion of this PIA could potentially result in technology changes*

No changes will be required

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

Industry Certifications

PII Mapping of Components (Servers/Database)

AcuStaf consists of **4** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by AcuStaf and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

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

Nurse_staff_dd_210	**Yes**	**Yes**	**Employee Name Employee Phone number**	**Staffing purposes**	All PII within the AcuStaf application is protected by Administrative, Technical, and Physical controls as noted within the AcuStaf ATO documentation and System Security Plan (SSP) and in accordance with NIST 800-53 standards adherence. Such controls include the use of access controls, need to know privileges, least privilege model implementation, and role-based access controls (RBAC). Furthermore, information encryption at-rest and in-transit is implemented. Physical security controls reside on the FedRAMP certification of Amazon Web Services GovCloud inclusions and are inherited.
PAID_DD_200	**Yes**	**Yes**	**Employee Home phone**	**Staffing purposes**	**All PII within the AcuStaf application is**

			Employee Email		**protected by Administrative, Technical, and Physical controls as noted within the AcuStaf ATO documentation and System Security Plan (SSP) and in accordance with NIST 800-53 standards adherence. Such controls include the use of access controls, need to know privileges, least privilege model implementation, and role-based access controls (RBAC). Furthermore, information encryption at-rest and in-transit is implemented. Physical security controls reside on the FedRAMP certification of Amazon Web Services GovCloud inclusions and are inherited.**
PAID_DD_450	**Yes**	**Yes**	**Employee name, date of birth, SSN, Employee Home Address**	**Staffing Purposes**	**All PII within the AcuStaf application is protected by Administrative, Technical, and Physical controls**

			Employee Sex		**as noted within the AcuStaf ATO documentation and System Security Plan (SSP) and in accordance with NIST 800-53 standards adherence. Such controls include the use of access controls, need to know privileges, least privilege model implementation, and role-based access controls (RBAC). Furthermore, information encryption at-rest and in-transit is implemented. Physical security controls reside on the FedRAMP certification of Amazon Web Services GovCloud inclusions and are inherited.**
HL7 ADT Messages	**Yes**	**Yes**	**Patient Name Patient SSN**	**Workload and ADT information for Staffing Purposes**	**All PII within the AcuStaf application is protected by Administrative, Technical, and Physical controls as noted within the AcuStaf ATO documentation and System**

					Security Plan (SSP) and in accordance with NIST 800-53 standards adherence. Such controls include the use of access controls, need to know privileges, least privilege model implementation, and role-based access controls (RBAC). Furthermore, information encryption at-rest and in-transit is implemented. Physical security controls reside on the FedRAMP certification of Amazon Web Services GovCloud inclusions and are inherited.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Information listed in section 1.1 is provided primarily through a nightly Secure File Transfer Protocol (SFTP) of Human Resources information and a continuous patient data feed that provides Admit, Discharge and Transfer dates, room numbers and beds (HL7) connection via a site-to-site connection with internal VA systems such as VistA.

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

Information listed in section 1.1 is provided primarily through a nightly Secure File Transfer Protocol (SFTP) of Human Resources information and a continuous patient data feed that provides Admit, Discharge and Transfer dates, room numbers and beds (HL7)connection via a site-to-site connection with internal VA systems such as VistA.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Not applicable

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?

PII is collected by the VA through Human Resource Systems and Patient Record Systems.

1.3b 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.

Not applicable

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.

Information is provided by the individual, supervisors, personnel records or obtained from their interation with the system and from other VA technology (IT) systems. Subjects of the record have access and amendment rights.

AcuStaf is not the source of the PII. PII is collected by the VA. It's not collected directly within AcuStaf.

1.4b 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.

N/A

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM (79VA10) is provided under Title 38, United States Code, section 7301(a).

Patient SSNs can be used as the unique identifier for HL7 Data received from the VA VistA ADT interface if the Patient ID is not provided. Patient information is collected for the use of nursing assignments to ensure equitable workload. Workload and employee information is used to automate VHA Directive 2010-034 and VHA Directive 1750. Executive Order 9397 gives authority to collect SSN and the authority for maintaining the information is Title 38 USC section 7301(a) which is in the VistA SORN 79VA10P2

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

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

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

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

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: Acustaf contains sensitive personal information – including social security numbers, names, and addresses on veterans, and VA employees. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm, or even identity theft may result.

Mitigation: Veterans Health Administration (VHA) deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within VHA to include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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.

Veterans or Dependents
- Name: Used to identify patient
- SSN: Used to identify patient

VA Employees

- Name: Used to identify staff
- SSN: Used to identify staff
- DOB: Used to identify staff
- Industry Certifications: Used to identify staff
- Address: Record for HR
- Phone Number: Record for contact
- Sex: Staff Identification
- Email Address: Record for contact
- Emergency Contact: Record for contact in case of emergency

AcuStaf Software is used to advance the VA workforce process management for its improved patient care through VHA directive 1351 compliance. AcuStaf Software is a workforce management technology that provides automated staffing, scheduling and labor management functionality. The application is web-based and provides the ability to create, view and edit staff schedules, track staff licenses and credentials, and generate management tracking and variance reports. The staffing and scheduling functionality includes time and attendance automation, as well as personnel scheduling. AcuStaf allows definition of employee positions, skill levels and credentials, and required hours. Categories for time and attendance hours include compensatory time, overtime, regular time, holiday, sick and vacation time. The reporting function includes more than 200 standard reports and ad-hoc reporting is available at the data element level. The labor management functionality currently integrates with existing human resource and payroll systems.

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.

Patient and employee data is used in order for AcuStaf to produce analytics on schedule hours, staffing numbers and census numbers to account for staffing compliance, overtime, absence days, and credentialing.

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.

Not applicable

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?

Data in transit and at rest are protected via at-rest encryption and transport layer encryption, using FIPS-validated cryptographic algorithms.

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

Additional protections are built in to ensure that data security and protection follows NIST provisions. Measures such as at-rest encryption, stringent access controls, and least privilege model are implemented.

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

In accordance with OMB Memo <-06-15, AcuStaf has appropriate physical, technical and administrative safeguards implemented to protect such data from unauthorized access. These protections leverage government cloud approved datacenters by Amazon Web Services and offer a full suite of physical protections. Administrative safeguards are implemented as per AcuStaf policies and procedures, and technical protections are implemented in accordance with the AcuStaf active authority to operate, leveraging NIST 800-53 controls for security.

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 controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA Focused training; face-to- face training for all incoming employees conducted by the Information System Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

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

Criteria, procedures, controls and responsibilities for access controls are documented and predicated upon the principle of least privilege and role based access control models.

2.4c Does access require manager approval?

Yes

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

Access to PII is monitored and tracked through logging and auditing mechanisms within the application.

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

Shared responsibilities to safeguarding PII are between AcuStaf and the VA personnel accessing the 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

Information retained may differ from facility to facility. However, all facilities retain information based on national VA policies. Below is a list of information that may be retained. These include: Employee Name, Employee SSN, Employee Date of Birth, Employee Mailing Address, Employee Phone, Patient name, Patient SSN, Patient Sex

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.*

In accordance with the System of Record Notice for 70VA10 which covers this system, POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

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?

When managing and maintaining VA data and records, AcuStaf will follow the guidelines established in VA Record Control Schedule (RCS)-10.

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

When managing and maintaining VA data and records, AcuStaf will follow the guidelines established in VA Record Control Schedule (RCS)-10.

Records Control Schedule 10-1 (va.gov)

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2
Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2
When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

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

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

All IT system and application development and deployment are handled by VA Office of Information and Technology (OI&T). PII/PHI may be used for Alpha or Beta testing at the facility-level per VHA policy. In addition, staff training on functionality in the new or modified application. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. VA Research investigators may use PII for VA Institutional Review Board (IRB)-approved research, and there is no effort to minimize the use of PII for research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by AcuStaf or its individual facilities will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in Acustaf is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

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***
VHA	Identifiable data provides a way to identify the employee and ways to contact them in case of shift changes Dates are necessary to identify seniority and provide ways to distinguish levels of service and other rules, such as union rulesCost Unit, Cost Center, and Station Number are all equally significant as it helps identify what department is responsible for the	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	SFTP and HL7 link

	cost of work versus where the work is being performed and helps track where, why, and what employees are scheduled to be doing. Examples include when nurses float to other units, etc. Job Codeshelp identify what type of work an employee does (ex. direct patient care vs indirect patient care which can impact metrics for nursing hours per patient day) as well as what type of policies are associated to the specific employee. They also help provide inputs for position control. Hired hours and work agreements are important so that managers avoid over-scheduling or under-scheduling based on employee agreed hours. Pay is important as it helps provide information to estimate the cost of staffing decisions.		

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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: The sharing of data is necessary for staffing purposes. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Microsoft Outlook is also another tool that is used to share internal information within the organization. Risks are mitigated by using encryption methods to share sensitive information within the organization.

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: There is no external data sharing.

Mitigation: There is no external data sharing.

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 VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

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."

Notice is also provided in the Federal Register with the publication of the SORN 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA (12/23/20)

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

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.

Notice is also provided in the Federal Register with the publication of the SORN 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VISTA) Records-VA (12/23/20)

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

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."

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 Veterans' Health Administration (VHA) requests only the minimum necessary information to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

There is no penalty assessed if the Veteran chooses to withhold information however this may cause delays in care or benefits.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract.

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.

VHA permits individuals to give consent or agree to the collection or use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. If individuals are not willing to give information verbally then they are not required to do so. Individuals are made aware of when they must give consent when there is data collected about them through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements which are on forms that collect personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. If the individual does not want to give consent then they are not required to in most cases unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VHA obtains a specifically signed written authorization for each intended purpose from individuals prior to releasing, disclosing or sharing PII and PHI.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits and that the NOPP is mailed out when there is a major change. The VA also mitigates this risk by providing the public with two forms of notice as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record Notice. Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided.

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.***

The VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. Each VHA Privacy Act system of records notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. VHA permits individual to obtain access to or get copies of their PII, and this is outlined in VHA policy such as VHA Directive 1605.01 Privacy and Release of Information. Individuals must provide a written request for copies of their records to the VHA facility Privacy Officer for medical records or the System Manager for the Privacy Act system of records as outlines in the notices. The request will be processed by VHA within 20 work days. The Department of Veterans' Affairs has also created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at: https://www.myhealth.va.gov/index.html Veterans and other individuals may also request copies of their medical records and other records containing personal data from a medical facility's Release of Information (ROI) office.Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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).

N/A

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.

N/A

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.

VHA has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA

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.

Veterans and employees are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:File an appeal File a "Statement of Disagreement"Ask that your initial request for amendment accompany all

future disclosures of the disputed health information Information can also be obtained by contacting the facility ROI office.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above to request edits to their personal medical records and other personal records retained about them.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran or an Employee may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: The Notice of Privacy Practice (NOPP), which every patient receives when they enroll for care discusses the process for requesting an amendment to one's records.
VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet (MHV) program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features.

In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended when appropriate

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.

Active Employees in approved T&LS have default access to the system. The T&Ls that utilize AcuStaf must first be added by an approved administrator to the VistA export, otherwise the data is not sent for employees or patients. This is documented in training and implementation materials.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

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?

N/A

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.
Z

Security levels are assigned to users based on their authorization, these can include no access, read only access or the ability to make changes. System level controls dictate if certain data can be updated by users with access to make changes.

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.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. This includes VA contractors are acting as nursing staff.

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 and VA contractors acting as nursing staff who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to PHI must complete the VHA mandated Privacy and HIPAA Focused training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05/05/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 07/12/2023
5. *The Authorization Termination Date:* 01/08/2024
6. *The Risk Review Completion Date:* 05/19/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

AcuStaf currently retains an ATO with the VA. Terms / Conditions for Authorization: Short-term ATO Granted. All findings must be remediated or have a documented remediation plan with an updated POA&M. Refer to the AO Requirements report for additional information on the findings. The system is classified as Moderate.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The AcuStaf system is a Commercial off the Shelf (COTS) product that is used by the VA as a managed service. Each implementation is private cloud deployment within Amazon Web Services GovCloud.

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.*

AcuStaf completes contract templates as specified by a facility's assigned contracting officer. The contracts establish expectations around the handling of PII/PHI. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (Pll), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of Pll.

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.

While AcuStaf leverages the Amazon Web Services GovCloud infrastructure, AcuStaf does not offer infrastructure as a service model for customers to fully control and/or lease infrastructure components.

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.

AcuStaf completes contract templates as specified by a facility's assigned contracting officer. The contracts include principles about VA Information and Information System Security/Privacy; Access to VA Information and VA Information Systems; Information System Design and Development; Information System Hosting, Operation, Maintenance or Use. Providers are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (Pll), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of Pll.

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

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

Not Applicable

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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**
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: 2023.09.01 15:54:14 -04'00'

Privacy Officer, Nancy Katz-Johnson

THOMAS ORLER

Digitally signed by THOMAS ORLER
Date: 2023.09.05 20:21:00 -05'00'

Information System Security Officer, Thomas Orler

SHEILA OCHYLSKI

Digitally signed by SHEILA OCHYLSKI
Date: 2023.09.06 09:24:45 -04'00'

Information System Owner, Sheila A. Ochylski

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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