Privacy Impact Assessment for the VA IT System called:

AIDIN: Web-Based Post-Acute Care Referral Management System

VA NY/NJ Integrated Healthcare System Network
Veterans Health Administration

Date PIA submitted for review:

March 15, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jackson Chin	Jackson.chin@va.gov	718-741-4055
Information System Security Officer (ISSO)	John Ferratella	John.ferratella@va.gov	(315) 560-4363
Information System Owner	Harris Khan	Harris.Khan2@va.gov	(202) 664-6577

Abstract

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

- The post-acute care referral management solution/system will provide a comprehensive care transition tool enabling hospital staff to efficiently transition medically ready Veterans from acute to post-acute care. The system will track post-acute care provider response to how they manage different illnesses in their healthcare facilities and nursing homes and their performance metrics (e.g., quality of care provided and Veteran satisfaction with the care they received).

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 name of the IT system is AIDIN: Web-Based Post-Acute Care Referral Management System. The IT system is owned by MRG, Inc (DBA AIDIN). AIDIN has ownership or control of this IT system. The business purpose of the IT system and how it relates to the agency mission is as follows: The solution shall encourage staff to follow an 'open market' search of interested partners on every referral; automatically assigns deadlines and marks delayed tasks as overdue in real-time through every step of placement;

generates advanced Veteran choice tools that highlight Medicare and real-time quality and satisfaction data for all available provider partners; and through patient and provider partner follow up and surveying, allows partner providers to establish their performance reputation against key criteria prioritized by VISN 2 leadership.

The exact number of veterans whose information will be collected and stored in the AIDIN system is unknown at this time. However, all veterans requiring post-acute care placement following a hospital discharge will be impacted. The veteran information collected is required and vital to ensure appropriate placement/treatment in a post-acute care setting. This information includes: name, SSN, DOB, gender, personal mailing address, personal phone number(s), emergency contact information, health insurance beneficiary numbers, current medications, previous medical records, medical record number, diagnosis. The AIDIN system conducts information sharing via a one-way communication. VISN2 staff/case manager inputs veteran information into the AIDIN system. VISN2 already has an existing BAA in place for sharing of PHI/PII information. Additionally, AIDIN is currently in the process of obtaining legal authority to operate the IT system through the FedRamp process.

At this time, no changes to business process or technology will be required with the completion of this PIA document. Furthermore, the IT system is not in the process of being modified; and a SORN does not exist for this IT system

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)

PII Mapping of Components

AIDIN: Web-Based Post-Acute Care Referral Management System 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 AIDIN: Web-Based Post-Acute Care Referral Management System and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

Internal Database Connections

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**
VistA	*Yes*	*Yes*	*name, social security number, date of birth, personal mailing address, personal phone numbers, emergency*	*To be used to obtain medical record information for appropriate patient placement in a post acute care setting*	*Data is fully encrypted behind the VA firewall. Additionally, VISTA users require access and verify codes as well as specified menus and*

			contact information, Health Insurance Beneficiary Numbers Account numbers, Medical Record Number Current Medications, Previous Medical Records, Medical Record Number, Gender		*keys to access PHI/PII*
VBMS	*Yes*	*Yes*	*name, social security number, date of birth, personal mailing address, personal phone numbers, emergency contact information, Health Insurance Beneficiary Numbers Account numbers, Medical Record Number Current Medications, Previous Medical Records, Medical Record*	*To be used to obtain disability/compensation for appropriate patient placement in a post acute care setting*	*Data is fully encrypted behind the VA firewall. Additionally, VBMS users require specific log in credentials to access the VBMS system*

			Number, *Gender*		

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.

- Social Workers will input patient information into AIDIN system for placement; and send any supplemental documents required for appropriate placement.

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.

- VISN2 staff will set up a HL7 ADT feed to programmatically provide the majority of required information. Social workers will input additional required patient information into AIDIN portal. Access is given only to the pertinent staff involved in patient referrals for post-acute care placement

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.

- All ADT feeds undergo testing prior to go-live to ensure accuracy and eliminate data corruption as outlined in the AIDIN implementation testing criteria. User social workers review all information before processing a record.

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

- A BAA and 6500 form are on file. Additionally, the Enterprise Risk Assessment will be done as part of the intake process through OIT

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:

AIDIN recognize the risks inherent in managing sensitive information and maintains a holistic privacy policy document. With regards to the characterization of the information, there are risks in collecting unnecessary information and sharing it unnecessarily across VA staff or partners, failing to collect veteran consent or properly managing the quality of the data.

Mitigation:

AIDIN only collects the information necessary to fulfill the business obligations contracted by the VA. Each data element is purpose specified and reviewed with every integration to ensure its utility and need.

AIDIN only divulges or shows information to users who need to see it, implementing controls around timing, status and user to ensure only required staff engage with sensitive patient information.

AIDIN relies on hospitals staff at the VA to use AIDIN's compliant patient choice tools which provide patients the opportunity to identify where their information may be shared.

All sensitive patient information is fed directly and verified directly from the VA source. Regular testing and maintenance on all inbound feeds ensures all data is complete and accurate. Users may also review and affirm or fix any information erroneously captured in the feed itself.

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.

Name:

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate/determine if provider facility has the capability to meet the care needs of the patient

Social Security Number:

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate/determine if provider facility has the capability to meet the care needs of the patient

Date of Birth:

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate/determine if provider facility has the capability to meet the care needs of the patient

Personal Mailing Address:

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Personal Phone Number(s):

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Emergency Contact Information (Name, Phone Number, etc. of a different individual)

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Health Insurance Beneficiary Numbers Account numbers

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Current Medications

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Previous Medical Records

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Medical Record Number

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the patient

Gender

- ✓ Information is required by receiving provider to identify the correct patient requiring placement and evaluate if provider facility has the capability to meet the care needs of the 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

- AIDIN does not perform any analysis, manipulation or changes to veteran information. All newly derived information is related to business processes only and not any patient-related information.

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?

- Data is encrypted in transit and at rest.

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

- SSNs are treated specially and are completely optional for inclusion. If they are included, SSNs are only exposed to reserved confirmed care providers and hidden through logic to all other users throughout the placement process.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

- All PHI and PII for Aidin applications and information systems is forced over SSL/TLS endpoints (TLS 1.2). Aidin uses a FIPS 140-2 validated cryptographic module - AES 256 bit.

- Data at rest is encrypted too. Each cryptographic key is segregated from the data it encrypts. The cryptographic key will be kept on a separate disk which itself will be encrypted. All mounting/unmounting events for the key volume are logged and made auditable to ensure key/data separation in the event of a security incident. Encryption protocol/key length – AES-256 bit.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information? There is no SORN in existence for this software

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project? Yes
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.

- VA Social workers are granted access to Aidin by VA administrators. All access to veteran information in Aidin is tracked and recorded and auditable. Aidin as well as its users are responsible for following PII safeguards and best practices.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

- All data elements identified in 1.1 are expunged according to the timelines outlined below in 3.2 – name, address, contact info, policy numbers, etc. No information considered PII is retained beyond the timelines outlined below in 3.2 – metadata like timestamps etc. are retained for reporting.

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.

- PII for veterans without records in Aidin is expunged 7 days after the veteran's hospital discharge. If a veteran has a referral record in Aidin, PII on that referral will be expunged 1 year after the last activity on that patient. All de-identified information and records remains available for auditing.

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.

- All database, server configuration, etc. are maintained indefinitely until the records control schedule is established by the National Archivist.

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

- All records are digital and are digitally cleared nightly in a programmatic script.

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

- PII is never used in testing. All testing and development environments are de-identified and contain zero PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:
Privacy Risk:
AIDIN recognize the risks inherent in managing sensitive information and maintains a holistic privacy policy. With regards to the retention of information, there are risks in retaining information when its usefulness is completed such as exposing old data or leaking irrelevant or old information.

Mitigation:

AIDIN retains the minimum amount of data from a content and a temporal perspective. AIDIN automatically tracks and removes old data at specific milestones in the workflow journey to ensure no information if held onto unnecessarily using scripts and other automated intelligent processes.

AIDIN purges old information by removing patient records who never receive services in the AIDIN platform, deidentifying patient records older than 1 year old, and updating out of date information with new information from live VA feeds. Aidin application screens as well as the databases that power them store only the content and the time period of information to serve the required workflows.

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***
VA CPRS - VistA	*Patient records and census, ADT feed*	*name, social security number, date of birth, personal mailing address, personal phone numbers, emergency contact information, Health Insurance Beneficiary Numbers, Account numbers, Medical Record Number Current Medications, Previous Medical Records, Medical Record Number, Gender*	*VPN tunnel HL7 ADT Feed*
VBMS	*To be used to obtain disability/compensation for appropriate patient placement in a post acute care setting*	*name, social security number, date of birth, personal mailing address, personal phone numbers, emergency contact information, Health*	*VPN tunnel HL7 ADT Feed*

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***
		Insurance Beneficiary Numbers, Account numbers, Medical Record Number Current Medications, Previous Medical Records, Medical Record Number, Gender	

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

Follow the format below:
<u>Privacy Risk:</u> The VA understands that certain risks are inherent in sharing data internally among staff, among them erroneously sharing data with staff who do not need access.

<u>Mitigation:</u> Only staff directly involved in patient discharge workflows will have access to the system. Access is managed by admin users who retain ability to review, remove and add access.

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***
Designated post-acute providers	Referral for post-acute services	name, social security number, date of birth, personal mailing address, personal phone numbers, emergency contact information, Health Insurance Beneficiary Numbers Account numbers, Medical Record Number Current Medications, Previous Medical Records, Medical Record Number, Gender	Contract with AIDIN allows permission to share Veteran placement information with community partners	Timed secured online portal access

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

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

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

Follow the format below:
<u>Privacy Risk:</u>

Aidin recognizes the risks inherent in managing sensitive information and maintains a holistic privacy policy document. With regards to the external sharing and disclosing of information, there are risks in granting access to unintended parties, intended but malicious parties using the data maliciously, and rescinding access if the work proceeds in another direction.

<u>Mitigation:</u>

Aidin relies on VA hospital staff to specifically direct if and where to share sensitive information. Aidin has built in tools for staff to identify the name, location, and contact information for partners they wish to contact through Aidin. They can update contact information in real time to ensure they are sending the right info to the right place.

VA users can rescind access to patient information at any time. Access is automatically rescinded throughout the workflow process when access is no longer necessary.

All records are audited and trackable so all access, edits, sharing and other actions are fully audited. The Activity List details every action, view, and more taken on an Aidin workflow.

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.

- No notice specific to collection of this information is used. However, most clients have a universal notice to inpatient patients informing them of where their information may be shared while under the care of the inpatient team. Generally, referrals to post-acute services are included in that scope and may be considered notice.

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

- Individuals do not have the opportunity to decline to provide information because it is necessary to provide case management services for safe discharge.

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

- No

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:

AIDIN recognize the risks inherent in managing sensitive information and maintains a holistic privacy policy. With regards to providing notice surrounding this data, there are risks in accidentally sharing information without a patient's consent.

Mitigation:

AIDIN relies on VA hospital staff to "choice" veterans or provide them with visibility into the options available for their care and the ability to direct if there is anywhere they do or do not want their information shared. This "patient choice" workflow is best practice and required to properly use the Aidin solution. Aidin provides tools to enable staff to audit and track their patient choice compliance.

Patient choice compliance ensures patients are polled before their information is shared through Aidin.

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.

- Access will be granted to users through a portal via system administrator

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.

- Procedure to correct erroneous information is to contact Aidin Support team via online chat, phone or email who can review, correct, and collaboratively investigate the source of the error for preventative resolution.

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.

- VA CPRS/integration team managing the HL7 feed will be the primary contact for correcting incorrect or missing information

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

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

- Any patient can gain access to their information in Aidin through a formal request from a client administrator. Should a patient have any concerns related to their case management services, in conjunction with case management leadership Aidin can make available to patients information about their referrals and records. This is not in the course of normal business.

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

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

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

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

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

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

Follow the format below:
<u>Privacy Risk:</u>

AIDIN recognize the risks inherent in managing sensitive information and maintains a holistic privacy policy. With regards to access, redress and correction of the information, there are risks related to the default access by hospital staff to the system as well as reliability of the source of information

<u>Mitigation:</u>

AIDIN allows users and hospital staff and administrators to share with owners of sensitive information if they have a record in Aidin relating to them. In fact, patient choice best practices will necessitate 'choicing' a patient before their record is created.

Aidin further mitigates risks by mirroring existing data about the patient in the EMR, limiting the opportunity for erroneous data or mismatching data between Aidin and the source EMR.

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.

- VISN Social Work Executive will work with facility POC to identify appropriate staff needed access to the software. Identified staff must be involved in patient discharge process to quality for access to the discharge software/solution. This information will be shared with AIDIN Chief Operating Officer/Integration Team for access.

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.

- Contractors will not have access to the system

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.

- TMS training on VA privacy and information system provided to all staff by default

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.***

- FedRamp process is still on-going. IOC date is 4/21/2023

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.

- Yes, but currently going through FedRamp review
- The cloud provider is AWS (Amazon Web Services) and the cloud model is SaaS (software as a service)

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.

- Will be determined as part of the FedRamp process.

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.

- Ancillary data such as logs, usage and other metadata is owned by AIDIN.

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.

- FedRamp authorization is still on-going

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).

- No, the system doesn't utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

JACKSON CHIN 137269

Digitally signed by JACKSON CHIN 137269
Date: 2022.12.06 13:11:57 -05'00'

Privacy Officer, Jackson Chin

John J Ferratella 130985

Digitally signed by John J Ferratella 130985
Date: 2022.12.07 12:55:23 -05'00'

Information System Security Officer, John Ferratella

HARRIS KHAN

Digitally signed by HARRIS KHAN
Date: 2022.12.08 09:43:54 -05'00'

Information System Owner, Harris Khan

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).