Privacy Impact Assessment for the VA IT System called:

Data and Analytical Support for Healthcare (DASH)

Veteran Health Administration (VHA)

VHA Innovation Center

Date PIA submitted for review:

07/24/2023

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	*Kamilah.Jackson@va.gov*	*513-288-6988*
Information System Security Officer	Amine Messaoudi	*Amine.Messaoudi@va.gov*	*202-815-9345*
Information System Security Officer	LaWanda Wells	*Lawanda.Wells@va.gov*	*202-632-7905*
Information System Owner	Angela Gant-curtis	*Angela.Gant-Curtis@va.gov*	*540-760-7222*

Abstract

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

Data and Analytical Support for Healthcare (DASH) is an application environment for predictive analytics concerned with the improvement quality of care, safety, and value to Veterans. DASH is a collaborative innovation effort with the Office of Health Innovation and Learning. The system integrates opportunities aimed to improve accuracy and reduce administrative burden in applications where machine learning and artificial intelligence can be of tangible benefit. The system supports developers productionizing solutions and pairing high-quality predictive analytics with support structures to ensure high-quality and low-latency solutions. Platform services will provide resources for productionizing machine learning/artificial intelligence deliverables to include continuous improvement and process improvement. Developers will be able to create new services focused on decision support opportunities. DASH integrate additional data through application programming interfaces and partnership integration agreements. DASH is productionized in Amazon Web Services environment including, but not limited to: storage for data structures, model discovery, training, and a production environment for delivering insight to the clinicians and administrators. DASH provides services to internal clients to deliver analytical solutions to a diverse group of end users. DASH creates utilities that deliver insights into clinical workflow and administrative workflows which will require coordination with internal and external customers.

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.

Data and Analytical Support for Healthcare (DASH) - VHA Innovation Center

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

Data and Analytical Support for Healthcare (DASH) is a cloud hosted solution that uses a middleware, called Using Machine Learning to Audit Rx Benefits (UMLRx), to audit prescriptions for accuracy of benefit decisions for veterans that have been awarded service connection\special authority ratings. The DASH application will receive prescription information in the form of HL7 messages which includes copay determination information and disability rating information. UMLRx uses the information about the prescription, and the disability information to determine if the copay status is correct. An auditor will be able utilize the determination from UMLRx to intervene and properly set the benefits and financial records. The accuracy of billing information is a source of

many audits published by the Office of the Inspector General and impacts the credibility of the Department of Veterans Affairs.

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

VA Owned and VA Operated

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.

The Bureau of Labor and Statistics reports that up to 4.9 million Veterans service-connected status and medical information to include prescription data will be stored. The typical client is VAMC personnel and Auditors.

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

DASH receives "RDS_O13" HL7 Pharmacy/treatment dispense messages which are standardized messages containing information about the patient, prescriptions, copay status, and warnings. DASH will also acquire disability ratings. The information is used to evaluate if a prescription is erroneously entered as a service connected or a non-service connected.

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

The system consists of a predictive model and middleware that calls other VA systems as well as the model. The other VA systems are VA Profile (to pull disability rating) and MPI Master Persons Index (to pull correct identifier for VA Profile). Information will not be shared with other systems, but results will be used to make interventions in Veterans Health Information Systems and Technology Architecture (VistA).

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.

DASH is not operated in more than one site. DASH is centralized in VAEC.

3. Legal Authority and SORN

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

Patient Medical Records -VA (SORN 24VA10A7)

https://www.oprm.va.gov/privacy/systems_of_records.aspx

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf - Authority for Maintenance of The System: Title 38, United States Code, Sections 501(b) and 304.

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 Vista system is not in the process of being modified and a SORN exists. The current SORN 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

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

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

Completion of the PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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)

Prescription outpatient identifier, Prescription IEN, ordering provider IEN, Ordering Provider Name, verifying provider IEN, and Verifying Provider Name

PII Mapping of Components (Servers/Database)

DASH consists of three (3) key components (servers). Each component has been analyzed to determine if any elements of that component collect PII. The first server, MLLP receiver, receives the HL7 message from Health-Connect, and sends parsed data to the 2nd server, the Middleware. The Middleware reaches out to VA Profile to receive disability information. The 3rd server, the Model, does not receive any PII or PHI. Final results are stores in our own internal database, which contains no PII or PHI. The type of PII collected by DASH 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
Health-Connect	Yes	Yes	RECEIVED: Names, SSN, DOB, Phone Numbers, Personal Mailing	The class I software is designed to include PII,	Encryption, 2-factor authentication,

			Address, Medication, Race/Ethnicity, Military History/Service, Integrated Control Number (ICN), Prescription outpatient identifier, Prescription IEN) SEND: Acknowledgement Message and that does not have any PHI or PII just the IP addresses in the message.	our system requires the information to be sourced from this software.	
VAProfile	Yes	Yes	SEND: Integrated Control Number (ICN) RECEIVED: Service connection, special authority, and Disability Information.	The class I software is designed to include PII, our system requires the information to be sourced from this software.	Encryption, 2-factor authentication,

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?

Incoming HL7 data is pushed to our system from VistA, via a Health Connect OPAI interface. This data is used to call MPI to pull the correct identifier, and VA Profile to pull disability rating.

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.

No external sources are used. Data from VistA, MPI, and VA Profile are needed for accurate predictions.

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

Our system creates a score but does not rely on analysis from other sources.

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?

Incoming HL7 data is pushed to our system from VistA, via a Health Connect OPAI interface. This data is used to call MPI to pull the correct identifier, and VA Profile to pull disability rating.

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.

All information collected is electronic.

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.

DASH receives data from two definitive sources of data. Incoming data to our gateway is derived from the electronic health record in the form of an HL7 O13 message that is an outpatient pharmacy order. The information in the HL7 message is standardized. The information in the HL7 message is event driven, when a provider enters an outpatient pharmacy order the translation of the order into the HL7 message occurs and that message is delivered to the pharmacy automation for use in filling

the prescription. If this data is inaccurate or corrupt the HL7 message will trigger a fault in our application and move the record to a SQS where the issue with the record will be triaged with logs.

On a monthly basis, the records that are evaluated within DASH are exported and combined with other data for reporting and trending. All HL7 messages received should be trackable back to the medical record, and data in analytical databases. This external validation step would identify any discrepancies. If any discrepancies were to originate from the VistA system, a Service Now ticket would be created for evaluation by the national teams responsible for the maintenance of the outpatient pharmacy automation interface, VistA, or Computerized Patient Record System (CPRS).

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.

The system does not check for accuracy by accessing a commercial aggregator of information

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

Patient Medical Records -VA (SORN 24VA10A7)
https://www.oprm.va.gov/privacy/systems_of_records.aspx
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
Authority for Maintenance of The System: Title 38, United States Code, Sections 501(b) and 304.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: DASH system deals with decisions of pharmacy billing decisions. The system does not store any PII or PHI. PII and PHI are used in transit from VistA to DASH system, but the application does not store or log any PII. What is sent from VistA is a standard HL7 message and is not custom to our application. A possible risk is that PII collected is improperly logged or intercepted in transit.

Mitigation: DASH system will perform monthly review of logs to verify that PII and PHI are not logged. If found as part of the application's monthly audits a notification of a breach will be sent to the Privacy Officer, System Owner and Information System Security Officer, and any offending code will be remedied. The appropriate procedure for notification and assessment of the breach will be followed.

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.

Model inputs are: drug name without dose, VA classification, and disability rating. To pull this information, we also use local drug identifier (to get drug name), and ICN to pull back disabilities.

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.

The system uses a predictive model to determine from drug name, VA classification, and disability rating(s) whether a given prescription should be charged a co-pay. The model generates one score for

every disability rating the Veteran may have and it also generates one score for the set of disability ratings.

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.

The system itself does not update any existing records but is used in making interventions.

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?

Messages in Simple Queue Service (SQS) are encrypted, messages are encrypted in transit (over HTTPS inside the VA network), and any storage is in a DB with encryption. All services are within our VPCs within the VAEC and must be accessed with a PIV or inside the VA network.

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

The HL7 message includes SSN and ICN. The HL7 is parsed for the information required and then securely deleted. The HL7 is not included in system logs.

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

There are technical safeguards to guard PII/PHI. No user can access DASH without permissions to AWS Gov-cloud which is control by VAEC. Any data that is imported into the environment uses approved methods for data transfer; and any data that is exported outside the secure environment can do so only utilizing approved methods for data transfer as documented in the tables below.

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?

All PII that comes through the system are pushed from Health-Connect.

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

The access to DASH system is control by VAEC following established procedures for granting elevated permission and through the use of security groups to control what users can access in the cloud. We do not manage access.

2.4c Does access require manager approval?

The application manager is responsible for submitting tickets to VAEC to assign users to the appropriate user roles to limit access.

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

Yes.

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

The Technical Team on DASH is responsible for assuring access to PII is safeguarded and that proper controls are in place to prevent the leaking of PII. The DASH system does not store PII.

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

Patient disability information (Service Connection/Special Authority), related service connection information, Prescription outpatient identifier (Prescription IEN), and facility, are retained in the DASH database. The information is retained temporarily, less than 30 days.

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.*

Model scores are only retained for a period of one year. Application logs are maintained for a period of 30 days. DASH receives a copy of the prescription order but does not maintain or update the patients' medical record.

DASH is not an archival system. The DASH system/application does not store PII long-term. All PII maintained in a Privacy Act system of records has a retention period identified in the SORN (i.e., Medical Record-VA: 24VA10A7) which is published in the Federal Register. VHA retains the accounting of disclosures for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted.

Record disposition refers to the transfer of records to a records storage facility, transfer of permanent records to the National Archives, the destruction of records, and other appropriate actions to dispose of records. The Record Control Schedule (RCS) 10-1 contains retention and disposition requirements for VHA records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority.

The VHA RCS 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records, states the retention period and disposition requirements. The actual defined period will be different depending on the specific record type. VHA Health care facilities do not set record retention periods or disposition authority for PII, nor do they set policy for data destruction. VHA health care facilities are to comply with the VHA RCS 10-1. https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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.
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?

The system of record is the Patient Medical Record. The data used to conduct the predictive analytics will remain in the Patient Medical Record, unchanged. The data will be retained in accordance with the Records Control Schedule.

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

The archived audit logs are kept for six years by the VHA as required by the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act as outlined in paragraph 35c (4) of VA Handbook 1605.1. Records control schedule (RCS) 10-1 provides the parameters for retention and destruction of data. RCS 10-1 is approved by NARA.

VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3

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

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.

DASH is not a record system and does not maintain, or store PII/PHI and there is no sensitive data for disposal. This system of record is the patient medical record.

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.

DASH does not conduct research, testing or training.

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 contained in DASH 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 breach.

Mitigation: DASH will delete records as soon as possible when no longer needed for processing. DASH has automated record deletion. The Patient Medical Record remains the system of record where data is stored.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration VistA	To provide prescription billing data	System Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (**Work with your System ISSO to complete all Privacy Risk questions inside the document this section**).*

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

Follow the format below:

Privacy Risk: There is potential privacy risks for the application layer logs to capture errors containing PII and PHI.

Mitigation: Ensure logging software does not record PII or PHI and logs are scrubbed before sending it to the application monitoring platform (Datadog).

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: No external sharing and disclosure of data.

Mitigation: Since no information is shared externally, no risk to mitigate.

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.

There is no new information being collected by the system. Data in DASH is pulled from VistA and VA Profile to create predictions. All of our information comes through VistA. Our system relies on what notification VistA sends and does not store any PII.

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

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of PHI/PII to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. The NOPP includes any use and/or disclosure of PHI/PII from VistA, CPRS and interfaced IT systems and solutions used for treatment, payment and/or health care operations. The most current NOPP is found here https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

24VA10A7 - Patient Medical Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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.

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of PHI/PII to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. The NOPP includes any use and/or disclosure of PHI/PII from VistA, CPRS and interfaced IT systems and solutions used for treatment, payment and/or health care operations. The most current NOPP is found here https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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 cannot decline providing information in DASH since the data is derived from VistA and VA Profile. However, if an individual chooses not provide data elements as part of care this would impact the ability receive information in DASH and to create scores for Veterans. While Veteran, patient or beneficiary may choose not to provide information to VHA, this may preclude the ability of VA to deliver healthcare and benefits due to those individuals.

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.

Yes, individuals may request in writing a record restriction limiting the use of their information by filling out a written request. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out. Individuals can request further limitations on other disclosures. A Veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. 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 NOPP 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 where

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 PHI and PII.

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: DASH does not issue notices to individual however, there is a risk that an individual may not receive the NOPP that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to VHA for treatment.

Mitigation: This risk is mitigated by providing the NOPP when Veterans apply for benefits and enroll for healthcare. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

DASH does not make changes to individual billing records. DASH does not make changes to individual billing records. DASH does not make changes to individual billing records.

If an individual (i.e., Veteran) is requesting access to one's own records, they may complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealtheVet program, VA's online personal health record using a premium account. More information about MyHealtheVet is available at https://www.myhealth.va.gov/index.html. In addition to the procedures discussed above, the SORNs listed in the Overview section of this PIA addresses record access, redress, and correction.

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).

DASH is a system application to provide data to the VAMC pharmacy billing teams to increase billing accuracy. The VHA Medical Record remains the system of record, from which DASH obtains data for use with performing data analytics to provide results back to Pharmacy Service. DASH is not a system of record.

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.

DASH does not store information at the individual user level.

A Veteran may request copies of billing information via Release of Information and receive copies of their health records following the process above in 7.1a.

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.

Data is not being collected by the system, as it relies exclusively on data from VistA and VA Profile.

VHA has a documented process for individuals to request inaccurate PHI/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 VHA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a signed 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 contains information on Contesting Record Procedure which informs the individual who to contact for redress. The NOPP 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.

Individuals are required to provide a signed written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. The NOPP also informs individuals how to file an amendment request with VHA.

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 individuals should use the formal redress procedures addressed above.

A formal redress process via the amendment process is available to all individuals whose information is maintained in a Privacy Act SORN.

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 incorrect information is in the health record resulting in improper diagnosis, treatment, and billing. Additionally, there is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their record via the amendment process.

Mitigation: The risk is mitigated by providing Veterans with access to their health information via requests submitted to Release of Information or premium account access through MHV. In addition, providing the Veteran with the NOPP which outlines the rights to request copies, restriction, and amendment to their health information.

The 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 My HealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where 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.

DASH system lives in a VAEC cloud environment, and an individual will need to submit a ticket with VAEC to be added to the system account. VA employees must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities.

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?

There will be no external users to the system.

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

There is an administrative role for developers, and a read-only role for users to pull scores. Users submit access requests based on need to know and job duties. These requests are submitted for VA employees, contractors and are processed through the appropriate approval processes. Once inside the system, individuals are authorized to access information on a need-to-know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

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.

The DASH contractors will have access to the system and PII. During development and Maintenance, the contractors will need access to PII for debugging purposes.
Also, there is a signed BAA on file.

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 Privacy and Health Insurance Portability and Accountability (HIPAA) focused 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 in the contract clarification of the mandatory nature of the training and the potential penalties for violating patient privacy.

Contractors are provision to access VA network and resources by the appropriate contract authority with the same requirements as VHA employees. As appropriate to the needs of the contract, contractors will complete a Business Associate Agreement (BAA) or Non-Disclosure Agreement (NDA) for review by the Office of General Council (OGC) and signed by all parties.

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 contractors must complete trainings through TMS: Privacy and HIPAA Focused Training (Course#:10203) and VA Privacy and Information Security Awareness and Rules of Behavior (WBT) (Course#:10176).

All VA employees and contractors 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 Protected health information or access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused required training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* TBD
2. *The System Security Plan Status Date:* TBD
3. *The Authorization Status:* TBD
4. *The Authorization Date:* TBD
5. *The Authorization Termination Date:* TBD
6. *The Risk Review Completion Date:* TBD
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.*** DASH Initial ATO Prospective date is (10/01/2023)

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), 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)*

Yes, the DASH system lives entirely in a VAEC AWS cloud environment which is FedRAMP approved.

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.*

Yes, PII and other data are owned by the VistA, VA Profile, and VAMCs. The DASH application does not how any ownership rights over the data.

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.

No

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.

AWS, as the cloud provider, is responsible for the security of hardware and low-level infrastructure. VAEC, as the system administrator, is primarily responsible for network security and user/developer access controls. The DASH team is responsible for application-level security and data encryption.

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 to DASH.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2023.09.20 10:52:52 -04'00'

Privacy Officer, Kamilah Jackson

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2023.09.20 11:45:17 -05'00'

Information Systems Security Officer, Amine Messaoudi

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
Date: 2023.09.20 10:14:02 -05'00'

Information Systems Owner, Angela Gant-curtis

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).

VHA Notice of Privacy Practices

Patient Medical Records -VA (SORN 24VA10A7)
https://www.oprm.va.gov/privacy/systems_of_records.aspx

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf - Authority for Maintenance of The System: Title 38, United States Code, Sections 501(b) and 304.

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