Privacy Impact Assessment for the VA IT System called:

Digital Health Pathway for Care Discovery (DHP-CD)

Veteran's Health Administration (VHA)

VHA Office of Healthcare Innovation and Learning

Date PIA submitted for review:

02/08/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Andrew Vilailack	andrew.vilailack@va.gov	(813) 970-7568
Information System Owner	Andrew Fichter	Andrew.fichter@va.gov	(240) 274-4459

	Name	E-mail	Phone Number
Record Officer	Tony Mallet	Tony.mallet@va.gov	(202) 382-4918

Abstract

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

Digital Health Pathway for Care Discovery (DHP-CD) is an early-stage testing and evaluation framework for novel sources and modes of consumption of Patient-Generated Health Data (PGHD). The DHP-CD Engine enables Veterans to register their connected devices (i.e., Fitbit) and grant or revoke permission for the VA to download new patient generated health data (PGHD). The DHP-CD Engine downloads patient-generated health data for enrolled Veterans, transforms it from vendor formats into standardized representations, and stores that data in composable, reusable Data Products. These PGHD Data Products will be visualized for clinicians at the point of care (alongside the electronic health record (EHR), adding context and intelligence to inform and enrich the clinician's 360 view of the patient). DHP-CD is intended to be a short-term assessment and trial framework for any given PGHD source or usage; in future, successful sources or usages of PGHD will be promoted out of DHP-CD and into other platforms if it is decided to implement them at large scale and/or over long timelines.

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.

Digital Health Pathway for Care Discovery (DHP-CD) - owned by the Office of Healthcare Innovation and Learning (OHIL)

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

To provide a rapid-assessment framework for novel sources and usages of Patient-Generated Health Data (PGHD) within the VA

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

VHA Office of Healthcare Innovation and Learning (OHIL)

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.

Present scope is 10-100 individuals. These will be VHA patients who are using consumer and home-medical devices outside of VA, and who have agreed to share the Patient-Generated Health Data (PGHD) on these devices with the VA for quality-improvement purposes.

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

The system imports Patient-Generated Health Data (PGHD) from third-party device vendors. For our initial pilot, the only vendor will be Fitbit, and the PGHD retrieved will include exercise calories spent, dietary calories consumed, hours of sleep, and heart rate. This information will be presented in a dashboard for the patient's care team.

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

PGHD is fetched from the device vendor (Fitbit) via HTTPS GET operation. The retrieved PGHD is transformed into a standard format and commingled with patient demographic information from CDW including name, date of birth, and last four characters of SSN, and stored in the HDAP/Rockies data lake for viewing with a Microsoft Power BI dashboard. There is no means of direct egress for the data once retrieved and stored.

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.

Interactive user access with the system is read-only via Microsoft Power BI. We leverage security controls within HDAP/Rockies and Power BI to grant dashboard access only to authorized clinicians. All assets of the framework are 100% cloud-based, so the system is accessible from all VA sites.

3. Legal Authority and SORN

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

VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). 2021-24368.pdf (govinfo.gov)

AUTHORITY: Title 38, United States Code, Section 501.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN will not require an amendment or revision and approval. The SORN covers cloud usage.

D. System Changes

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

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

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

Completion of this PIA will not result in circumstances that require 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 (Last four digits only)
- ☒ 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)

• Activity, Sleep, Heart Rate, and Dietary Calorie metrics as received from a Fitbit wearable device

PII Mapping of Components (Servers/Database)

The **Digital Health Pathway for Care Discovery (DHP-CD)** consists of **two** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the **Digital Health Pathway for Care Discovery (DHP-CD)** 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
HDAP CDW Replica	Yes	Yes	Name, DOB, last four of SSN, Activity, Sleep, Heart Rate, and Dietary Calorie metrics as received from a Fitbit wearable device	Enabling patient search in the clinician dashboard	Only available as search terms in a report/dashboard
HDAP CDW Replica	Yes	Yes	ICN	Used to associate imported PGHD with the relevant patient	Never visible or exportable by users

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?

The information is imported directly from the HDAP/Rockies replica of CDW tables SPatient and PatientICN.

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.

We are using the VA's authoritative copy of patient demographic information for search and display purposes in a Power BI dashboard.

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

The system generates a dashboard/report UI containing the patient's PGHD for viewing by the patient's care team.

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?

Patient demographic information is retrieved from a CDW replica via direct database query, as part of the automated ETL process for newly-retrieved PGHD.

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.

No form

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your

organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

For patient-generated health data (PGHD), access tokens used to retrieve the data are associated with the ICN of the Veteran who has agreed to share data. The retrieved PGHD is then associated with the ICN from the access-tokens collection. This is done on a one-by-one basis, so there's minimal risk. We retain a copy of the raw data as received from the vendor, and have the capability to validate the accuracy of imported and transformed data products against that.

We leverage the data quality and integrity controls that undergird CDW and its HDAP replica:

For Veteran PII imported from CDW replicas, we leverage the data quality and integrity controls that undergird CDW and its HDAP replica. For that, please see this response from the HDAP/Rockies team:

> Whether and how often information stored in the system is checked for accuracy.
> - Daily, we check RCV and successful loads, no full check on every table every day. Only on exceptions do we check accuracy. We have developed accuracy / DQ checks but is only run manually.
>
> Is information in the system checked against any other source of information (within or outside our 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?
> - We only check against SQL202 only, due to that is our source
>
> 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.
> - No instances have been reported. Daily we check RCV and successful loads, no full check on every table every day. Only on exceptions do we check accuracy. We have developed accuracy / DQ checks but is only run on a manually.
>
> Do we have any information on how data integrity is assured in the CDW replicas?
> - Independent teams look at independent processes/replicas; there is no total oversight of all replicas within the teams.

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.

No third-party sources are used for information accuracy checks.

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

Digital Health Pathway for Care Discovery falls under the boundary of the VA LightHouse DI Authority to Operate (ATO) as a minor app and is authorized until 11 Oct 2023. Users of DHP-CD will receive informed consent of data collection and uses of data upon log-in to DHP-CD.

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

The authority for ‘‘VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). 2021-24368.pdf (govinfo.gov) is Title 38, United States Code, Section 501.

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:
DHP-CD collects and stores PII and PHI for Veterans. Therefore, a risk exists that data could be accessed by individuals who do not have a need to know or who intend to use the information in a way that is not authorized and therefore unlawful.

Mitigation:
In order to safeguard Veterans' PII and PHI stored in DHP-CD, we've implemented the following protections:

- **Data is read-only.** No tooling exists which enables users to update or delete DHP-CD data.
- **User interface leverages Active Directory security.** The user interface for DHP-CD is Microsoft Power BI, as hosted by VA BISL. Only users who have been deliberately added to a new, single-purpose Active Directory group will have access to the Power BI report(s).
- **No means of data egress is supported.** Veterans' PII and PHI stored in DHP-CD can be viewed using Microsoft Power BI, but there is no means to export, download, or otherwise transfer DHP-CD data out of the HDAP/Rockies data lake.

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.

The information collected and maintained will be used to view patients' PGHD (Patient-Generated Health Data) in a Microsoft Power BI report at the point of care. This report will be used by VA clinicians to assess the quality and relevance of the PGHD, in support of the DHP-CD mission of providing rapid, easy assessment of new sources and usages of PGHD. There is no external use case for this information.

Name: Used to identify the Veteran.
Social Security Number: Used as a unique Veteran identifier.
Date of Birth: Used to identify the Veteran.
ICN: Used as a unique Veteran identifier
Activity, Sleep, Heart Rate, and Dietary Calorie metrics as received from a Fitbit wearable device: Used to collect PGHD information about the Veteran.

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.

DHP-CD imports previously un-utilized Patient-Generated Health Data (PGHD) from consumer and home-medical devices outside of the traditional clinical space to assess the quality and utility of the data, and to experiment with and develop use cases for that data as envisioned by and co-created with VA clinicians. Although we do envision future use cases where large scale data analysis will contribute to DHP-CD mission goals, at our current pilot scale we have not yet designed or implemented any such use cases.

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.

DHP-CD imports previously un-utilized Patient-Generated Health Data (PGHD) from consumer and home-medical devices outside of the traditional clinical space to assess the quality and utility of the data, and to experiment with and develop use cases for that data as envisioned by and co-created with VA clinicians. This data is stored in its own repository which is only used by DHP-CD and surfaced to VA clinicians through custom data visualizations. No existing VA datasets or records are appended, modified, or deleted by the DHP-CD. The mission of DHP-CD at pilot scope is to give clinicians a tool to assess the *data retrieved and the tools that display that data*, rather than to inform or modify their determination of the *patient's health*.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit from the public internet (patient PGHD) is encrypted in transit (HTTPS) and the data in transit contains no PII. Once the PGHD is retrieved into the VA's IT estate, there is no means of egress provided. Data at rest is stored within the Azure Data Lake Services (ADLS) environment of the HDAP/Rockies platform, and we leverage all available protections offered by that platform.

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

We store the last four characters of the patient's SSN for use as a search term in the clinician dashboard. The full SSN is never stored in DHP-CD, and it is never shown in a user interface, report, or dashboard.

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

All PHI and PII will be stored in HDAP/Rockies within the VA Enterprise cloud, will leverage the privacy and security protocols of VA HDAP/Rockies, and will be adherent to the VA security protocols, including data encryption. All database data shall be encrypted with the industry standard AES-256 encryption algorithm. The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer.

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?

Read-only access will be granted on an as-needed basis to VA clinicians who are granted controlled access to DHP-CD. Controls are in place to ensure that anyone with access to the PII will have conducted mandatory online information security and Privacy and HIPAA training as stated in Section 2.3c.

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

Yes. DHP-289 Power BI Access Control from Rockies - Dept of Veterans Affairs-External - MAX Federal Community

2.4c Does access require manager approval?

Users granted access to the system and the access controls they are granted is currently determined by the System Owner and/or their Delegates. Access to the system requires approval of the System Owner and/or their Delegates.

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

We collect usage metrics of the Power BI dashboard(s) for purposes of measuring usage and adoption. Although we don't currently have tools which enable us to monitor usage of the report by individual clinicians, we believe that that capability does exist within the usage data itself.

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

Access to DHP-CD is given to approved users (including VA clinicians, System Owner, and their Delegates). DHP-CD leverages VA Enterprise practices for enabling access to the system.

Section 3. Retention of Information

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

3.1 What information is retained?

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

PII: Name, SSN (only last four characters), DOB, ICN
PHI: Activity, Sleep, Heart Rate, and Dietary Calorie metrics as received from a Fitbit wearable device

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.

Due to the innovative nature of DHP-CD, the aforementioned PII and PHI data will be retained for a series of discrete pilots for a minimum timeframe of 6 to 12 months, or until the team determines the data is no longer needed (per General Records Schedules GRS20, item1c and GRS24, item6a).

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

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

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

Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

3.*3b Please indicate each records retention schedule, series, and disposition authority.*
General Records Schedules (GRS) | National Archives

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.

As no hard copies are created, simple digital deletion is sufficient to ensure permanent destruction of VA's copy of the data. The data exists on the VAEC and will not be stored on magnetic media. Digital deletion entails that the data will be deleted from their file location and then permanently deleted from the deleted items or Recycle bin in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization.

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.

Although the PGHD retrieved is anticipated to have meaningful value in a research context, we have not yet begun developing that use case. When use cases at an aggregate/population level (such as research) are developed, we intend to remove PII from the interface for any research data surfaced.

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(s): Data is retained by DHP-CD for at least 6 to 12 months, during which it is at risk of unintended access. There is a minimal risk that information could be retained for longer than needed.

Mitigation: Only the minimum PHI and PII necessary is retained, minimizing the magnitude of harm. Access controls are in place to limit access. These controls will be in place for the entire duration that data is retained in the system. Information necessary to impose retention rules is stored within the data and metadata.

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***
VistA	Correlate patient PII to imported PHI, in order to support search and display in the user interface	Patient Identity fields: ICN, First Name, Last Name, Date of Birth, SSN	Read directly from CDW replica in HDAP (not egressed from HDAP)

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: DHP-CD will display PII and PHI in PowerBI dashboards for access-authorized VA clinicians in which the read-only interface will visualize data. To the DHP-CD team's awareness, this does not introduce new risks, being that there is no writeback capability (e.g., DHP-CD will not share information with VistA) and no data egress capabilities from PowerBI. There is a minimal privacy risk that unsponsored internal sharing of PII and disclosure could occur if the information is not encrypted and if the information is not limited to authorized users.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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***
Fitbit Fitbit Web API	Data received from Fitbit via the Fitbit Web API to HDAP/Rockies	Activity, Sleep, Heart Rate, and Dietary Calorie metrics as received from a Fitbit wearable device	We are receiving (never transmitting) data in accordance with Fitbit's public ToS.	HTTPS GET We are receiving (never transmitting) data in accordance with Fitbit's public ToS.

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:

Privacy Risk: There is minimal risk that during external connection and data transit from the Fitbit Web API, that a data could be intercepted in transit.

Mitigation: Per NIST-compliant HTTPS encryption standards and VA 6500 handbooks, data in transit (i.e., in the request or response) from the Fitbit Web API is not identifiable and cannot be traced back to the Veteran nor their PHI & PII.

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.

DHP-CD provides notice of information regarding the VA Privacy Policy on the va.gov webpage where Veterans can connect their device. Veterans are also notified that by providing consent to collection of information, their Fitbit data including activity, sleep, heart rate, and dietary calorie metrics will be shared and displayed in a dashboard for VA clinician use.

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

Notice is also provided in the Federal Register with the publication of the SORN:
VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). 2021-24368.pdf (govinfo.gov)

AUTHORITY: Title 38, United States Code, Section 501.

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

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

Notices are provided to the Veteran when they connect their Fitbit device to va.gov. The notice delineates the purpose of DHP-CD, the reason for data sharing, privacy of data, intended uses of data, and obtains user consent.

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

Notice is also provided in the Federal Register with the publication of the SORN:
VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). 2021-24368.pdf (govinfo.gov)

AUTHORITY: Title 38, United States Code, Section 501.

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.

Yes. DHP-CD is only able to access Veteran data that the veteran has explicitly agreed to share. The Veteran may withdraw sharing permission through either of two means: (1) They may execute a "Disconnect" operation in the Connected Devices section of VA.gov, which both deletes the credentials needed for VA to access that data and also informs Fitbit that the Veteran has withdrawn permission; or (2) they may manage their Fitbit account at fitbit.com, and there they also have the opportunity to tell Fitbit directly not to share data with VA.

DHP-CD is currently a pilot program, and the Veterans and clinicians participating are volunteers; there is no reward for participation and no penalty for not participating.

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.

At present the only use of the information is for review by VA clinicians. The Veteran is informed of this usage at the time they choose whether to register their device, and they may deny that usage by not connecting.

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: DHP-CD is only able to access Veteran data that the veteran has explicitly agreed to share however there is a risk that they may ignore it or that they are not notified that their data is being collected.

Mitigation: To mitigate the above privacy risks, the Veteran has to manually initiate the sign-up process. If the Veteran does not sign-up, the data cannot be made available for transfer from the

Fitbit Web API. Veterans that do sign-up are sufficiently notified on va.gov of the data that is collected and the intended uses of such data, in layman's terms and in legalese. Veterans are additionally notified of their rights to decline to provide information and cease use of Fitbit device connection. Notice is also provided in the PIA and the SORN.

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.***

Access procedures are specified in the SORN: RECORD ACCESS PROCEDURES: Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

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

N/A

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

N/A

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1,

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

Veteran PII is sourced from canonical VA systems which have their own mechanisms for remediation. In the case that imported PHI is found to be incorrect, the cause of the problem can be identified and fixed, and any affected data can be re-imported. In accordance with the SORN: Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

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.

At pilot scale, we will be processing all support requests through a single purpose support email address. Any data correction will entail finding and fixing errors in the import process, and so this is the most efficient route for any requests for correction to take.

In accordance with the SORN, Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

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.

N/A

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The procedures for access, redress and correction are listed in the SORN and this PIA. The data collected is intended to be used by a patient and their care team; patients will have the opportunity to access the data with, and request redress or correction from, a VA clinician known to them.

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.

Any individual being granted access to the system will be a clinician who becomes authorized to view the Power BI report containing the Veteran PHI. All clinician users will have had mandatory information security and HIPAA training as a condition for prior authorization to access to the EHR system. As we are running a pilot, those individuals will be a very small pool (5-25) of clinicians who have individually volunteered through meetings and emails. Actual management of clinician access is documented here: DHP-289 Power BI Access Control from Rockies - Dept of Veterans Affairs-External - MAX Federal Community

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?

We do not currently plan to provide access to users from other agencies outside VA.

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.

All Production users of the system have read-only access. Developers and other maintainers will only be able to adjustment or otherwise modify the data through update scripts which will maintain a robust audit trail using version control and execution logging.

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 system was built by a contractor, Thoughtworks, in partnership with VA Office of Healthcare Innovation and Learning and the VA Office of the Chief Technology Officer. In Production, contractors as well as VA employees will have only read-only access to the data. Providing the contractors who built the system with read access is necessary for verification, maintenance, and updates in the running system. The contractor, Thoughtworks have a BAA and NDA on file, in compliance with Prime Contract Number VA118-16-D-1015.

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 parties working on the system have completed mandatory training on VA's security and privacy controls and policies. Employees with access to the system are also required to take annual VA Rules

of Behavior training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11 October 2022
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 11 October 2022
5. *The Authorization Termination Date:* 11 October 2022
6. *The Risk Review Completion Date:* 8 December 2022
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.***

N/A

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)*

This system will use the VA Enterprise Cloud (VAEC).

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.*

N/A

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.

N/A

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.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.02.16 14:03:45 -05'00'

Privacy Officer, Nancy Katz-Johnson

Digitally signed by ANDREW VILAILACK
Date: 2023.02.16 12:52:54 -05'00'

Information System Security Officer, Andrew Vilailack

ANDREW FICHTER

Digitally signed by ANDREW FICHTER
Date: 2023.02.17 08:30:18 -05'00'

Information System Owner, Andrew Fichter

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).

VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). 2021-24368.pdf (govinfo.gov)

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices