Privacy Impact Assessment for the VA IT System called:

VetChange Clinician

Veterans Health Administration (VHA)

National Center for Post-Traumatic Stress Disorder (NCPTSD)

eMASS ID 1276

Date PIA submitted for review:

05/06/24

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	(503) 721-1037
Information System Security Officer (ISSO)	Mark J. McGee	James.McGee5@va.gov	(520)358-3237
Information System Owner	Liston, Dena	Dena.Liston@va.gov	(304)886-7367

Abstract

The abstract provides the simplest explanation for "what does the system do?"

VetChange Clinician is the clinically integrated version of VetChange, with patient- and provider-facing functionality for integration into clinical care. The expanded application offers clinical provider accounts and dashboard, patient enrollment and registration, patient account administration, provider assignments to patients with access to their data. VetChange Clinician is an online self-management program for active-duty military, veterans, non-veterans, and non-service members who are concerned about their drinking. It offers tools and information to help build skills to better manage drinking and Post-Traumatic Stress Disorder (PTSD) related symptoms. Those who use the intervention do not need to have a clinical diagnosis of any kind. The intervention was tested in a research study and shown to help decrease symptoms for both problems.

In order to use VetChange Clinician most effectively, end-users (veterans) have the option to provide the following types of information: goals to cut down on or stop drinking; answers to questions about drinking patterns, thoughts, feelings, and moods; the importance that changing their behavior has for the user, and pros and cons of change; situations the user defines as risky for increasing their drinking; coping strategies and plans for drinking, stress, sleep, and anger.

The information that the user enters into the optional assessments in VetChange Clinician will be automatically compared and computed by the database to present the user with helpful summary information. VetChange Clinician consists of nine self-guided modules that include education and tools to help the end-user change their drinking behavior. End-users create an account to log in, preferably daily, to log the number of drinks they have consumed, work with VetChange Clinician tools, and track their progress towards meeting their change goals. End-users that need alternative information about managing drinking, or mental health concerns are provided with a list of military, government, and non-government resources they can reach out to. This web application uses an SQL database as its storage system.

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. What is the IT system name and the name of the program office that owns the IT system?

The System name is VetChange Clinician, and the owning organization is the National Center for Post-Traumatic Stress Disorder (NCPTSD).

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

VetChange Clinician is an online self-management and clinician assisted program for active-duty military, veterans, non-veterans, and non-service members who are concerned about their drinking. It

offers tools and information, and clinical guidance to help build skills to better manage drinking and Post-Traumatic Stress Disorder (PTSD) related symptoms.

C. Who is the owner or control of the IT system or project?

VetChange Clinician is owned by the National Center for Post-Traumatic Stress Disorder (PTSD).

2. Information Collection and Sharing

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

In the first year of operation, there will be approximately 100 individuals entering information into the VetChange Clinician system. The clients will include veterans and VA providers (VA clinicians and/or contractors).

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The information collected in VetChange Clinician will include veteran name, age, email address, login.gov Sec ID, and veteran Health and Drinking Information (quantity, dates, moods, additional drug use). The purpose is to help veterans–on their own or with a VA clinician–build skills for better managing their drinking and Post-Traumatic Stress Disorder (PTSD) related symptoms.

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

VetChange Clinician collects PIV information from VA IAM system as well as Login.gov information for the purposes of authentication. VetChange Clinician does not share this information with any other system.

G. If 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?

The VetChange Clinician system is solely hosted in the VA Enterprise Cloud (VAEC) environment.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

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 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.

SORN 173VA005OP2 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP)" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf. Authority for maintenance of the system: Title 38, United States Code, Section 501.

4. System Changes

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

No. We are not anticipating any business process changes to VetChange Clinician.

K. Will the completion of this PIA potentially result in technology changes?

No. We are not anticipating any technology process changes to VetChange Clinician.

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- **Veterans**
  - VA SEC ID
  - Name
  - Age
  - Race
  - Ethnicity
  - Education Level
  - Mental Health Information
  - Veteran's Drinking and Substance Abuse Information
  - Veteran's Era of Service
  - Veteran's PTSD Information
- **VA Employees**
  - Name
  - VA SEC ID
  - VA Email Address
  - VA VISN Information
- **VA Contractors**
  - Name
  - VA SEC ID
  - VA Email

PII Mapping of Components (Servers/Database)

VetChange Clinician consists of one (1) key component(s) (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VetChange Clinician 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
VetChange Clinician Web Application Server	Yes	Yes	• Personal Email Address • VA SEC ID • Name • Age • Race • Ethnicity • Education Level • Mental Health Information • Veteran's Drinking and	• Personal Email is collected for communication purposes. • VAEC SEC ID is for login purposes. • Name is for clinician's records • All other information is for clinical	Encryption at rest Amazon RDS encrypted DB is the industry standard AES-256 encryption algorithm to encrypt data on the server. SSL for any communication I/O.

			Substance Abuse Information • Veteran's Era of Service • Veteran's PTSD Information	diagnostic and care purposes.	

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

1.2 a 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 entered by veterans and VA clinicians who interact via the system. The information helps veterans, and their providers, work together in developing skills to help veterans better manage drinking and Post-Traumatic Stress Disorder (PTSD) related symptoms.

1.2 b 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 additional information nor inputs from external data sources are required besides the data inputs provided by VetChange Clinician end-users (veterans).

1.2 c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

No.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3 a 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?

Veteran information is entered by the veterans themselves. Clinician PIV information is collected via IAM/PIV. All information transmissions by the Veteran and Provider are performed over an SSL connection between the client web browser and VA Web Server.

1.3 b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

VetChange Clinician does not use any forms subject to the Paperwork Reduction Act.

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.

End-user information provided by veterans, which is collected and stored in the VetChange Clinician application, is checked for accuracy through reviews conducted by VA clinicians and authentication against the VA IAM directory to verify user identity (e.g., Name, VA SEC ID, VA Email address, VA VISN Info).

1.4 b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No additional information nor inputs from external data sources are required besides the data inputs provided by VetChange Clinician end-users (veterans).

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

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.

SORN 173VA005OP2 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP)" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf. Authority for maintenance of the system: 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: Due to the highly sensitive nature of this data, there would be a risk if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional harm may result for individuals affected.

Mitigation: The VA will only collect and secure the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance.

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 that 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.

• PII/PHI Data Element	• Internal Use	• External Use
• Email • Name	• Authentication	• None
• VA SEC ID • Sex • Age • Race • Ethnicity • Education Level • Mental Health Information • Veteran's Drinking and Substance Abuse Information	• Collected so that the Veteran can receive guidance on self-managing their drinking and PTSD, and for them to work with a VA clinician to manage these conditions.	• None

• Veteran's era of service Veteran's PTSD Information.		

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?

Clinicians using the VetChange Clinician system review patient progress throughout the system. Data collected from end-users (veterans) is utilized to establish goals to reduce drinking habits, track progress towards established goals in the form of daily check-ins / personalized feedback from VA clinicians and provide education to manage symptoms which contribute to alcohol consumption.

No additional analytical tasks are performed on data collected / stored by the VetChange Clinician system. Personalized review of end-user data is solely reviewed by VA clinicians to provide feedback.

2.2 b 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.

End-users (veterans) of the VetChange Clinician system enter their own data which is utilized to establish goals to reduce drinking habits, track progress towards established goals in the form of daily check-ins / personalized feedback from VA clinicians and provide education to manage symptoms which contribute to alcohol consumption. Information collected about the veteran is updated on their existing user record within the VetChange Clinician database.

New information about the veteran's drinking and PTSD symptoms are created and updated on their learning module records within the VetChange Clinician database.

The VetChange Clinician system does not use any previously unutilized data about any individual users.

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?

The VetChange Clinician SQL database uses encryption at rest. Amazon RDS encrypted DB instances the industry standard AES-256 encryption algorithm to encrypt data on the server. SSL is implemented for all data in transit.

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

The VetChange Clinician system does not collect SSN's.

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

The VetChange Clinician database uses Amazon RDS encrypted DB instances the industry standard AES-256 encryption algorithm to encrypt data on the server.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Onscreen displays of patient information (E.g., emails are anonymized.)

Regarding any information that may be produced outside the system (E.g., paper print outs), clinicians operate in accordance with HIPAA.

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.

2.4 a How is access to the PII determined?

Access to personally identifiable information (PII) within the VetChange Clinician system is role-based:

- **System Administrator**
  - The System Admin users have access to all user data.
- **VA Clinicians**
  - The VA Clinician users have access to their own patient's user data.
- **Veteran patients**
  - The veteran users have access to only their data.

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

- Criteria to access the system and associated data are:
  - VA clinicians that provide patient care.

- Vendors who maintain the system work under the authority of the National Center for PTSD. All vendors with access are authorized by the VA and carry active Work without compensation (WOC) status and active PIV cards.
- Veterans that receive patient care.

2.4 c Does access require manager approval?

The VetChange Clinician business owner gives blanket authority to the software vendor to access and maintain the system.

VA clinicians providing patient care have access to the VetChange Clinician system but are only provided access to view veteran profiles and data which have been assigned to them specifically.

Veterans (serving as end-users) solely have access to view and edit information within their dedicated account, following the account registration/creation process.

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

No.

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

The VA business owner Nicholas Livingstone and the software development vendors (EDC/Headspin).

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

- **Veterans**
  - Email, name, and SEC ID are collected for authentication and communications purposes.
  - Sex, Age, Mental Health Information, Race, Ethnicity, Education Level, Veteran's Drinking and Substance Abuse Information, Veteran's era of service, and Veteran's PTSD Information.
- **VA Employees (Clinicians)**
  - Name
  - VA SEC ID
  - VA Email Address
  - VA VISN Information
- **VA Contractors**
  - Name
  - VA SEC ID
  - VA Email Address

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.*

The VetChange Clinician system retains data in accordance with National Archives and Records Administration (NARA) retention period timeline requirements. Currently 6 years.

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?

VetChange Clinician follows the NARA General Records Control Schedule (GRS) 3.2, items 30 and 31. NARA General Records Control Schedule (GRS).

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

VetChange Clinician follows the NARA General Records Control Schedule (GRS) 3.21, items 30 and 31 with disposition authorities DAA-GRS2013-0006- 0003 and DAA-GRS2013-0006- 0004. NARA General Records Control Schedule (GRS).

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.

While VetChange Clinician end-user (veterans) records are retained in compliance with National Archives and Records Administration (NARA) retention period timelines, veterans can request that their user account, to include provided data inputs, be deleted / disposed of. Following receipt of a record disposal request, VA clinicians would delete the associate account and data inputs, providing

confirmation back to the end-user that the task is complete. "Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. When an end-user requests their account information to be deleted, the VetChange Clinician system administrator uses the user management dashboard to delete all the data entered by the user and any data associated with their account within the system. If the end-user / clinician relationship is ended, the data can be deleted using the same dashboard. Similarly, once the retention period is over, the user data can be deleted using the user management dashboard.

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.

The system will not be used for Research at this time. Real Veteran data is used for pilot testing and training with VA clinicians, but access will be restricted to those staff authorized to be participating in the pilot.

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: If data is retained for longer than necessary to fulfill its purpose, a greater risk of the data being unintentionally released or breached could occur.

Mitigation: To mitigate the risk posed by information retention time periods within VetChange Clinician, once a record is cleared for disposal, the system administrator disposes of the record and records disposal actions.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Identity Access Management (IAM)	Authentication	• Email address • Name • VA SEC ID • VA Email address	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• VA VISN Info	
Login.gov	Authentication	Email address, VA SEC ID	HTTPS

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: The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: To mitigate privacy risks associated with sharing authentication data elements with internal VA system / services, VetChange Clinician utilizes the Secure Sockets Layer (SSL) protocol for encrypting, securing, and authenticating communications sessions between the web browser (user interface) and web application server. Additionally, SSL is deployed to encrypt and secure intra-VAEC network connections between the VetChange Clinician system and VA services / systems used to authenticate users (VA IAM and Login.gov).

The implementation of SSL encryption provides mitigation protections against data tampering and protects the confidentiality and integrity of data-in-transit between the VetChange Clinician system and internal VA services / systems.

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***
None	None	None	None	None

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: VetChange Clinician does not share information outside of the Department of Veterans Affairs.

Mitigation: VetChange Clinician does not share information outside of the Department of Veterans Affairs.

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 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.

Terms of Service (ToS) are displayed during user account creation in the VetChange Clinician system. The ToS includes a specified notice which states the information types that will be collected on behalf of end-users (veterans) in the system, intended usage of the collected information, and information pertaining to the privacy and security of collected information. (See a copy of ToS in Appendix A below)

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

SORN 173VA005OP2 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP)" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf.

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

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

Notice is provided.

6.1 c 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.

Patients who use this system will have already provided "consent to treat" as part of normal clinic operations. The Terms of Service (ToS) additionally includes a specified notice which states the information types that will be collected on behalf of end-users (veterans) in the system, intend usage of the collected information, and information pertaining to the privacy and security of collected information.

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

SORN 173VA005OP2 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP)" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf. This document explains what SORN applies to information maintained in this system and how it may be used and disclosed.

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

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.

A user can decline to provide information and opt-out of using the VetChange Clinician system**.**

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Veterans wishing to use VetChange Clinician do have to give consent to use the system, provided in the form of accepting the VetChange Clinician Terms of Service (ToS). If they do not wish to consent, then they cannot use the system. The value of the system is working with a VA Clinician in managing behavior based on data input from end-users (veterans).

Individuals also have the right to request a restriction to the use of their information. The written 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 a facility Privacy Officer for review and processing.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that Veterans using the system do not understand how their information may be used.

Mitigation: The VetChange Clinician system displays applicable Terms of Service (ToS) which dictates information usage and the purposes for usage. The ToS specifies the data elements that will be collected on behalf of users and must be acknowledged and agreed to prior to moving forward with system usage. The ToS clarifies that requested information, which end-users (veterans) have the option to enter into the system, are used to provide feedback on drinking habits and how to reduce alcohol misuse/consumption which may result from Post-Traumatic Stress Disorder (PTSD) symptoms.

There is a common practice of providing the NOPP when Veterans apply for benefits.

Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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 https://department.va.gov/foia/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

All end-users (veterans) may access the information entered about them in the VetChange Clinician system.

Individuals seeking information regarding access to and contesting of records maintained under the 173VA005OP2 SORN 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)?

The VetChange Clinician system is not exempt from the access provision of the Privacy Act.

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

The VetChange Clinician system is not exempt from the access provision of the Privacy Act.

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.

All end-user (veterans) data input into the VetChange Clinician system is input by the end-user. Only end-users have read/write permission into the system to input information pertaining to their dedicated account. In the event that an end-user has identified inaccurate or erroneous information, they are able to edit and remediate the information that had been input as needed.

Veterans are also informed of their rights to request amendments to records about them in VHA Notice of Privacy Practice (NOPP).

Individuals seeking information regarding access to and contesting of records maintained under the 173VA005OP2 SORN 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.

Within the VetChange Clinician system, only registered and approved end-users (veterans) are authorized to input and/or edit submitted information. VA clinicians, and supporting VA contractors, only have read-only access when viewing end-user (veterans) information input into the system.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP).

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

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3.

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: In the VetChange Clinician system, end-users (veterans) must be invited to register and proactively input the information needed to facilitate account creation. Within the system, only end-users have the ability the ability to input information pertaining to their account / profile, while VA providers (clinicians and/or contractors) only have read-only access. The usage of the above data elements are prescribed in the VetChange Clinician Terms of Service (ToS).

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?

The system Admin gives access to clinician/provider and the clinician/provider invites patient via the VetChange Clinician application.

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?

No other agencies have access to the data in VetChange Clinician 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.

Within the VetChange Clinician system, there are only two roles prescribed for system usage, which include:

1. End-Users (veterans) who have read/write access to input and modify information pertaining to their specific account within the system.
2. VA providers (clinicians and/or contractors) which solicit clinical care services to educate Veterans, establish goals, and track progress to reduce drinking and substance abuse habits related to PTSD symptoms. VA providers only have read-only access to the system.

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.

VA contractors will have access to the VetChange Clinician system, each of whom functions under Work Without Compensation (WOC) status.

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.

VA Clinicians and VA contractors are required to pass the following VA TMA curriculum requirements:

- FISMA Reporting Curriculum
- Privacy and HIPAA
- VA Privacy and Information Security Awareness and Rules of Behavior (WBT)

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

In Process.

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)*

VetChange is Platform as a Service (PaaS) which will be hosted on VAEC MAP on AWS.

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.*

VetChange Clinician is hosted in the VA Enterprise Cloud (VAEC); thus, no further responses are required.

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.

VetChange Clinician is hosted in the VA Enterprise Cloud (VAEC); thus, no further responses are required.

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.

VetChange Clinician is hosted in the VA Enterprise Cloud (VAEC); thus, no further responses are required.

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).

VetChange Clinician is hosted in the VA Enterprise Cloud (VAEC); thus, no further responses are required.

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**
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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.05.14 08:40:14 -07'00'

Privacy Officer,

JAMES MCGEE

Digitally signed by JAMES MCGEE
Date: 2024.05.16 09:40:37 -07'00'

Information System Security Officer,

DENA LISTON

Digitally signed by DENA LISTON
Date: 2024.05.16 16:20:54 -04'00'

Information System Owner,

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; screen shot of a website collection privacy notice).

VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 173VA005OP2 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP)" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf.

VetChange Terms of Service:

VetChange Clinician is an online self-management program that enables mental health professionals ("providers") to directly incorporate their patients' use of VetChange Clinician into treatment. The goal of the clinical care that VetChange Clinician is based upon is to help Veterans and active-duty military learn skills to better manage their drinking and PTSD symptoms. Non-Veterans and non-Servicemembers can also use VetChange Clinician.

The Department of Veterans Affairs' National Center for PTSD ("we" or "us,") provides this service. In these Terms of Service, "your provider" means the mental health professional who invited you to work together in VetChange Clinician.

By signing up for an account on VetChange Clinician, you are acknowledging and agreeing to these Terms of Use that describe important cautions for you about using VetChange Clinician with your provider, and information about the privacy and security of your personal information.

DISCLAIMERS: WHAT YOU SHOULD KNOW ABOUT USING VETCHANGE CLINICIAN WITH YOUR PROVIDER

1. Your provider will be able to observe all the information you enter in VetChange Clinician if you agree to these terms and create a VetChange Clinician account that is linked with your provider. You or your provider may terminate this link at any time, and that will immediately disable your provider's access to your account and all your information. If the link to your provider is terminated, you may still use VetChange Clinician on your own as a self-guided program, and all of your information will still be there.

2. Except for the guidance your provider gives you, you will not have contact with other mental health professionals to guide you or answer questions about the information presented or your personal situation. If you feel that you need personal help, consult your provider or visit resources for information on finding more assistance.

3. VetChange Clinician is designed to help you gain control over drinking by either cutting down or stopping. If at any time while using VetChange Clinician you find that your drinking is increasing instead of decreasing, you could be at risk for experiencing more serious problems and you should consult your provider or seek other personal assistance.

   Some individuals may become physically dependent on alcohol if they have been drinking for a period of time. When a person is alcohol dependent, they may experience alcohol withdrawal if they suddenly stop drinking or drastically cut down. Symptoms of alcohol withdrawal usually begin within a few hours of decreasing drinking and may include: tremors, sweating, elevated pulse and blood pressure, nausea, insomnia, anxiety, seizures, and possibly delirium. Stopping or cutting down on your own can be medically dangerous if you are physically dependent on alcohol.

   If you suspect that you may be physically dependent on alcohol or you experience any withdrawal symptoms, please consult your provider or seek other professional help before trying to stop or cut down drinking on your own.

4. VetChange Clinician is focused on drinking, not drug use. If you are frequently or heavily using recreational drugs or are misusing medications (using more than prescribed by your doctor or using medications not prescribed for you), VetChange Clinician may not be suitable for you even if you are also having alcohol problems. Examples of recreational drugs include cocaine, marijuana, methamphetamine, heroin, or club drugs such as Ecstasy. Examples of commonly misused prescription drugs include pain killers (such as Oxycodone), tranquilizers (like Valium), stimulants (such as Adderall) or drugs to block withdrawal (like Suboxone).

   Regular use of drugs is likely to interfere with your ability to stop or cut down on drinking, and stopping without medical intervention could be dangerous to your health. If you want or need help for drug problems, please consult your provider or visit resources.

5. VetChange Clinician helps you learn new skills to manage moods and possible emotional reactions to serving in combat. If at any time while using VetChange Clinician you feel overwhelmed by your emotions or believe that you have symptoms that are worsening (for example, feelings of sadness are getting more frequent or intense), you should consult your provider or seek other professional assistance.
   If you feel at any time that you want to hurt yourself anyone else, go to the nearest emergency room or call 911. You may also call the Veterans Crisis Line at any time at 1-800-273-8255.

PRIVACY AND SECURITY OF YOUR INFORMATION

1. Information we ask you to provide when registering
   To use VetChange Clinician and grant your provider access to your information, you must register for a VetChange Clinician account by providing a user ID you create (it does not have to be your real name), your email address, your age and your sex. We use your email address to send you automated notifications about your use of the system. We use your age and sex to

provide you with automated personalized guidance. We also ask you to voluntarily enter your ethnicity and Veteran status, for group data about who is using VetChange Clinician. You may also opt to provide your mobile phone number to receive automated text messages about your use of the system.

If you do not want to provide your email address, you can register for a VetChange Clinician account without an email address at VetChange Clinician.org. This will enable you to use the program on your own, but you will NOT be able to link to your provider and grant them access to your information.

2. Information you may provide when using VetChange Clinician
   To gain the most benefit from VetChange Clinician, once you register you have the option to enter additional personal information such as a record of how much you drink, or your thoughts, feelings, and plans about cutting back or stopping your drinking. The main purpose for collecting this information is so we can provide feedback on your drinking and what it might mean for you, and also suggest new ways of approaching things that may help you decrease any alcohol misuse or trauma-related problems that may trigger drinking. Some of the information that is saved will be presented to you again in future sessions. Information that you enter into the optional self-assessment questionnaires will be used to present you with helpful feedback. We will also collect anonymous summary statistics about patterns of use on the tools and pages on VetChange Clinician, in order to improve the service.

3. How we protect your information
   Your participation and all your information will be kept confidential. Only authorized people (as explained in section 4 below) have access to your information.
   We use reasonable administrative, technical and physical security measures to help protect your personal information. These measures conform to generally accepted standards to protect personal information submitted to us during transmission and once it is received. However, because no security measures are perfect or impenetrable, and no method of data transmission can be guaranteed against any interception or other type of misuses, we cannot guarantee complete security for personal information provided. VetChange Clinician uses secure databases and servers to store your data, and all data is transmitted, stored, and processed in a secure environment. All of your information is protected by firewalls, encryption, authenticated access, physical access control, policies for technical personnel, and other means to prevent access by anyone who is not supposed to see it. All systems are patched, monitored and scanned routinely for vulnerabilities and intrusions. We do not employ third-party cookies or IP addresses to track behavior on the website.

   Your email address, and mobile phone number if you provide it, may tie your identity to the information you enter. Emails and text messages sent by VetChange Clinician are not encrypted and should not be considered secure. Because of this, we only send emails and text messages with general wording that doesn't mention alcohol or other specific health concerns, and only

refers to your provider by their name, avoiding any wording suggesting that they are a mental health professional.

It is also important that you help maintain the privacy of your data on VetChange Clinician by keeping your login email and password secret, and securing access to your email account and mobile phone number. If you are worried that someone else may be using your login information, please let us know immediately, or change your password yourself through the My Profile setting page.

4. Who has access to your information
   You have continual access to your own data, by entering the email and password you created at registration.
   In general, under federal law, identifiable health information is private. However, there are exceptions to this rule. In some cases, others may see your identifiable health information for purposes of administrative oversight, quality control, public health and safety, or law enforcement. VetChange Clinician administrators and contractors (computer programmers) will have access so that they may perform maintenance, troubleshooting, and updates to VetChange Clinician. We share your health information only when we must, and we ask anyone who receives it from us to protect your privacy. We will never sell, rent, or lease your information.

5. Browser Cookies and IP Addresses
   VetChange Clinician employs browser cookies to keep you logged into the website and to anonymously associate your browsing activity with your stored data in order to personalize the information you see. VetChange Clinician does not link browser cookies with any information you submit during your site visits.
   VetChange Clinician logs IP addresses, or the location of a computer on the Internet, whenever someone requests a web page from VetChange Clinician.org. For security reasons, VetChange Clinician records your logged IP address when your register for an account, and stores it in your data record. We do not use IP address logs to otherwise track your user sessions or behavior on our site, nor to personally identify you. We use IP addresses solely for security systems administration and troubleshooting purposes.

6. You may request your account be deleted at any time. There are two ways of having your account and information deleted from VetChange Clinician: You can request your account be removed and data be deleted via a request within the application or you can send an email to your provider. Once your account is deleted, all information you entered will be deleted from the system.

ACKNOWLEDGMENT AND AGREEMENT

By voluntarily providing information on VetChange Clinician.org you are consenting to the Veterans Administration's use and disclosure of that information in the manner described in these terms of use.

Please visit the contact page to reach a VetChange Clinician program administrator with questions about these terms of use.

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Directive 1605.04: Notice of Privacy Practices