Privacy Impact Assessment for the VA IT System called:

VEText Assessing

Veterans' Health Administration (VHA)

Office of the Chief Technology Officer (CTO)

Date PIA submitted for review:

August 14, 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)	Randall Smith	Randall.Smith@va.gov	319-338-0581 x636266
Information System Owner	Shane Elliott	Shane.Elliott@va.gov	909-503-2889

Abstract

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

VEText Assessing (VEText) is a VA-developed appointment reminder system that pulls appointment data from VistA and sends an appointment reminder text message through VA Notify to Veterans allowing them to either confirm or cancel their appointment. Providing appointment reminders encourages Veterans to attend their appointments and reduces the number of no-shows and rescheduled appointments. VEText enables the Veteran to text a response to cancel an appointment, providing an easy and convenient cancellation method and freeing up appointment times so that other Veterans are able to access care more quickly

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.

The system name is VEText Assessing (abbreviated as VEText) and it is owned by the Office of Information Technology (OIT).

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

The convenience of VEText for the Veteran increases the operational efficiency of VA by decreasing staff call volumes and automatically cancelling the appointment without staff intervention. VEText provides a technology within VA that has become standard practice in the private sector medical community.

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

VEText was developed entirely by the VA and is hosted and maintained on servers internal to the VA network. The name of the VA Administration is VHA, and the program office is the Office of the Chief Technology Officer.

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.

VEText is expected to store approximately 9 million unique Veteran records. The individuals are Veterans who receive care under the VA Healthcare System.

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

VEText is an SMS appointment reminder system that pulls appointment data from VistA and sends an appointment reminder (via third party Short Message Service (SMS) gateway) to the Veteran allowing them to either confirm, cancel, or view more details about their upcoming appointment(s). The VA-developed VEText software solution integrates with VA Profile to retrieve patient phone number and VistA for appointment information. VEText uses VA Notify to securely send and receive SMS text messages to remind Veterans of their appointments and allows for cancellation of the appointment by the Veteran. If the response is to cancel, the VEText software cancels the appointment in VistA. VEText was originally developed at the Loma Linda VA Healthcare System to address the high rate of patients not attending their scheduled appointments. Nationally, over nine million appointments go unused each year due to patient no-shows. In addition, almost 90% of Veterans have basic cellphones. The goal was to send automated reminder messages for upcoming appointments to patients via SMS text messaging. The system is configurable to send up to three reminders to patients before their appointment date/time. This software also facilitates patient-initiated cancellation of appointments, freeing the appointment up for another Veteran. VEText communicates with Veterans at medical centers with VEText enabled. VEText obtains patient internal entry number (IEN), patient cell phone number, and appointment information to include date and time from VistA to send the appointment reminders and retains that information for reporting purposes. VEText is currently available at all VHA facilities. VEText is configured and monitored at each VHA facility site with a web-based admin portal. The VEText Portal can be accessed on the VA network from any major internet browser (i.e., Microsoft Internet Explorer, Google Chrome, Apple Safari, etc.), allowing configuration of specific clinics to send messages for, reports, and other various settings. Communication from the device to the web server uses standard Internet protocols (e.g. HTTP/HTTPS). VEText uses a Mongo database to cache patient and appointment information and uses a SQL database to store configuration information for each clinic, text message templates, etc. VistA is the data source for Veteran appointment information and Veteran's cell phone number. Data is obtained using VistA Remote Procedure Calls (RPCs).VA Notify is a VA product that allows software developers to programmatically send and receive SMS text messages. VEText uses an HTTP Secure Sockets Layer (SSL) connection to securely send SMS messages to patients through VA Notify and to receive SMS responses from patients. Pusher is a commercial service employing a published/subscribed (pub/sub) business model. VEText uses Pusher to initiate a persistent web sockets connection. There is no sensitive information stored in the cloud environment. VEText only transmits PII over SMS to Veterans that opt-in to receive PHI/PII VEText messages. The only PII currently transmitted in the SMS message is Clinic name/Clinic friendly. VEText obtains ICN, patient cell phone number, clinic name, last four numbers of SSN, and appointment information to include date and time from VistA to send appointment related messaging and retains that information for reporting purposes. This information is also shared with the internal Microsoft Structured Query Language (MSSQL) Database used for VHA Support Service Capital Assets (VSSC) Reporting and VA Microsoft Power BI reporting. First name, phone number, appointment date and time, and clinic name (if patient opts-in) are sent to the Veteran VA Notify. If data was lost from this system, names and cell phones for Veterans could be obtained, but the system does not store full Social Security Numbers (SSN). Only PII/PHI collected and used by the facilities within the Boundary will be referenced in this document since the Boundary does not maintain, disseminate, or store information accessed by each facility. PII/PHI. The facilities within the Boundary collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, VBMS, BOSS/AMASS, etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

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

All information used by VEText is pulled directly from VistA, Master Person Index (MPI), and VA Profile.

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.

VEText is available to any VA site with access to VistA.

3. Legal Authority and SORN

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

VEText operates under the Privacy Act of SORN 79VA10. (https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf)

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

The current SORN covers cloud usage and storage and does not need to be updated at this time. The application operates in accordance with SORN 79VA10 (https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf)

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Appointment Date/Time, Clinic Name, COVID-19 Vaccination Interest/Status, VA Profile ID, VA Clinician Names.

PII Mapping of Components (Servers/Database)

VEText Assessing consists of 3 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 VEText Assessing 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
Application Server	No	No	• Phone Number • Name • ICN • Appointment Date/Time • Clinic Name • Last four of SSN • COVID-19 Vaccination Interest/Status	For sending messages and for reporting purposes.	Username, Password, Various levels of access, SSL encryption for transmission
MSSQL Server Database	No	Yes	• Phone Number • Name • ICN • Appointment Date/Time • Clinic Name • Last four of SSN • COVID-19 Vaccination Interest/Status	For sending messages and for reporting purposes.	Username, Password, Various levels of access, SSL encryption for transmission.
MongoDB Database	No	Yes	• Phone Number • Name • ICN • Appointment Date/Time • Clinic Name • Last four of SSN • COVID-19 Vaccination Interest/Status	For sending messages and for reporting purposes.	Username, Password, Various levels of access, SSL encryption for transmission.

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?

Phone number, name, ICN, appointment date/time, clinic name, last four of SSN, and clinician name are pulled directly from VistA. COVID-19 vaccination appointment or vaccination status comes from the CDW for vaccinations or vaccination appointments made within the VA. A response of VAX directly from the patient through the VEText SMS service indicates a vaccination outside the VA.

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.

Commercial aggregators are not used. Information is collected from individuals and/or EHRs to provide information relevant to appointments.

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

VEText uses PowerBI to generate relevant reports for VEText users and VEText product team to monitor the usage of the platform. VEText also generates reports internally for users to investigate the use of the system.

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?

VEText collects all necessary information using Remote Procedure Calls (RPC) from VistA.

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.

Information is not gathered on a 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.

VEText retrieves information from VistA in real-time. VistA is the system of record for patient information and appointments, which is identified by the ICN of the patient. This uniquely identifiable system information is used to ensure accuracy.

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.

Commercial aggregators are not used.

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 authority to collect the information in VEText is derived from the VistA system. The VistA System, and the VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), 304, and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a).
Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

- System of Record Notice - 79VA10 Veterans Health Information Systems and Technology Architecture - VA
    - https://www.oprm.va.gov/docs/SORN/Current_SORN_List_05_09_2023.pdf

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: Sending Clinic Name to Veterans via SMS messages. The system retrieves the information from VistA and sending the messages resides within the VA firewall and communicates with the SMS gateway provider via secure connections. However, the transmission of this information to the patient will be over cellular networks and unsecure as SMS has no method for encrypting messages.

Mitigation:

1. Control: Text messages containing clinic name will only be exchanged with patients that have expressly opted into VEText by completing an electronic consent. By completing this consent, the patient will acknowledge acceptance of the risks of sending and receiving unsecured text messages and exercising their rights of access.

    a. Risk Mitigation Action Implementation: Before sending text messages with clinic name to a patient, an opt-in text message will be sent to the patient including the risks associated with sending and receiving unsecured text messages. Veterans will be required to confirm via text message, and a follow-up authentication will be sent requesting the veterans date of birth. If the Veteran responds with the correct date of birth, the Veteran will be considered consented and enrolled in VEText.

2. Control: Text messages will be sent individually and only to the telephone number listed in the patient's medical record (VistA) and only after the patient confirms the telephone number is theirs and re-confirms annually.

    a. Risk Mitigation Action Implementation: Text messages will only be sent to the mobile number listed in the patient's VistA record only after the patient has verified the number belongs to them by responding to the enrollment consent with their date of birth. Additionally, an annual message will be sent to the patient requiring them to validate the number is still theirs by responding with their date of birth.

3. Control: The Veteran may opt out at any time by sending a text message reply to VEText.

    a. Risk Mitigation Action Implementation: The Veteran may opt out at any time by sending a text message with the word STOP to VEText via the designated phone number or by responding to any message received from VEText.

4. Control: Protected information under 38 U.S.C Section 7332 will NOT be sent via unsecure text messages to the patient.

    a. Risk Mitigation Action Implementation: Section 7332 information includes information pertaining to drug abuse, alcoholism or alcohol abuse, infection with HIV or sickle cell anemia. VEText will filter any appointment with a clinic name that includes these conditions and not send the reminder.

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.

Internal use of the information will be for reporting and routine scheduling functions performed by frontline VHA staff. External use of the information will be for the routing (Phone Number) and content (Appointment Date/Time and Clinic Name) of the appointment reminder sent to the Veteran; Patient name: Used as an identifier; ICN: Used as an identifier; Phone number: Used to send text message; Appointment date and time: Used in the body of the text message and as input to cancel the appointment if Veteran's response indicates to cancel; Clinic name: Used in the body of the text

message; COVID-19 Vaccination Interest/Status: Used in patient responses to COVID-19 Vaccination outreach messages.

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.

VEText creates trend-analysis, and relational analysis reports utilizing PowerBI software to analyze and display the data analytics in the form of visual graphs and charts, as well as sums, averages. These reports do not contain any PII/PHI and are only accessible on the VA-network.

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.

VEText does not create or make available any new or previously utilized information in regard to an individual Veteran.

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?

Access to the VEText Portal is controlled by VistA access and VA Single Sign On Internal (SSOi). Only users with a VistA account may access the VEText portal. In accordance with VA Directive Handbook 6210, all VEText users begin with the minimum level of access required to utilize the application. Additionally, VEText inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized to access in VistA. Access to additional VEText functionality can be requested by the VEText Facility Point of Contact (POC) or the VEText VISN POC which is reviewed and validated by VEText staff. VEText portal login information is logged. The system owner is responsible for ensuring these safeguards are in place and functioning.

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

VEText user access to SSN is limited to the Medical Center Electronic Health Records (VistA) the user is authorized to access in VistA and are only displayed in specific reports. Only the last four of the SSN is stored by VEText.

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

Access to the VEText portal is controlled by VistA access and VA Single Sign On Internal (SSOi). Only users with a VistA account may access the VEText portal. In accordance with VA Directive and Handbook 6210, all VEText users begin with the minimum level of access required to utilize the application. Additionally, VEText inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized for in VistA. Access to additional VEText functionality can be requested by the VEText Facility Point of Contact (POC) or VEText VISN POC which is reviewed and validated by VEText staff. VEText portal log in information is logged.

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?

Access to VEText PII is controlled by VistA access and Single Sign On Internal (SSOi). Only Users with a VistA account may access VEText PII. In accordance with the VA Directive and Handbook 6210, all VEText Users with the minimum level of access required to utilize the application.

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

VEText inherits VistA site access rules, ensuring each User can only access those Medical Center Electronic Health Records the User is authorized for in VistA. Access to additional VEText functionality can be requested by the VEText Facility Point of Contact (POC) or VEText VISN POC which is reviewed and validated by VEText staff.

2.4c Does access require manager approval?

Yes, VEText inherits VistA site access rules, ensuring each User can only access those Medical Center Electronic Health Records the User is authorized for in VistA. Access to additional VEText functionality can be requested by the VEText Facility Point of Contact (POC) or VEText VISN POC which is reviewed and validated by VEText staff.

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

Yes, VEText portal log in information is logged.

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

The system owner is responsible for ensuring VEText safeguards are in place and functioning.

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*

VEText Assessing processes the following information: Name; Phone Number; ICN; Appointment Date/Time; Clinic Name; Last four of SSN; COVID-19 Vaccine Interest/Status. Information is stored until the appointment event has occurred. Retention of this information is not beneficial beyond that event and is purged once the appointment event has occurred. The maximum retention period for any data processed is 14 days.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system,***

please be sure to list each of these retention periods*. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

VEText Assessing does not serve as an Electronic Health Record (EHR) or data repository. It would not be necessary for VEText Assessing to retain processed data beyond the time period in which it is used to assist in the appointment process. All data sourced by VEText Assessing is drawn from VistA which serves as the authoritative collection repository.

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

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

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

Yes

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

RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005–0004, item 020). RCS10–1, Item 2100.32100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006–0004, item 31).

3.4 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.

Data no longer necessary will be deleted from the database. Data contained in VEText is transitory and if deleted from VEText is retained within VistA. This is in accordance with RCS 10–1, Item

2000.2, DAA–GRS–2013–0005–0004, item 020 and RCS10–1, Item 2100.32100.3, DAA–GRS–2013–0006–0004, item 31.

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.

Any information shared for research will be de-identified and will not include Name and Phone Number. This will ensure the information is no longer PII. Any information shared for research will be de-identified and will not include Name and Phone Number. This will ensure the information is no longer PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VEText could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at

greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, VEText adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The VEText system ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the boundary to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration VistA	VEText Assessing gathers necessary information from VistA to send pertinent text messages.	Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN	Remote Procedure Calls (RPC)
Veteran's Health Administration VA Notify	VA Notify receives information from VEText to send messages to Veterans	First Name, Appointment, Date/Time, Clinic Name, Cell Phone Number	SSL Connection with Representational State Transfer (REST) application programming interface (API) and sends the messages by making an HTTP POST
CDW	VEText stores application configuration information and caches some VistA information.	Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status	Extract Transform Load (ETL)
Master Person Index (MPI)	VEText Assessing gathers the required information to enable it to query VA Profile.	ICN, VA profile ID	SSL Connection with REST AP
VA Profile	VEText Assessing gathers communication preferences to determine the channel to send messages to veterans.	VA Profile ID, Communication Preference, Phone Num	SSL Connection with REST AP

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 individuals to receive benefits at the VEText. 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: 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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the VEText. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.
All personnel accessing Veteran's information must first have a successfully adjudicated background screening or Special Agreement Check (SAC). This background check is conducted by the Office of Personnel Management A background investigation is required commensurate with the individual's duties.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter. This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORN 2020-28340.pdf (govinfo.gov)

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

The routine use provision of the Privacy Act functions as one of the exceptions to the statute's general prohibition against the disclosure of a record without the written consent of the individual to whom the record pertains.

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

Notice is provided to all Veterans who are eligible for care. The notice is also available at all VA medical centers as well as online:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Information used is previously collected and stored in VistA. 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. Patients do have the option to opt out of receiving appointment reminders from VEText. There is no penalty for opting out.

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.

VEText can include clinic name and patient first name in text messages. Patients will be presented with a consent and have the option of opting out of including this PII in the text message. Without consent they will get a text message that includes appointment date and time only.

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.
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.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. 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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

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

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practices (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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The system does not create any new patient information that the patient does not already have access to through the medical records system. All information that the system obtains is already available in the patient's medical records (i.e., VistA).

SORN for 79VA10 provides record access procedures: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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 system is subject to the access provisions of the Privacy Act.

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.

VistA is the electronic medical record database for VA and has an established process for release of information to obtain a copy of or make changes to information in VistA.

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.

The system does not create any new patient information that the patient does not already have access to through the medical records system. All information that the system obtains is already available in the patient's medical records (i.e., VistA). VistA is the electronic medical record database for VA and has an established process for release of information to obtain a copy of or make changes to information in VistA.

SORN for 79VA10 provides record access and contesting procedures: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

The system does not maintain health records outside of VistA.
SORN for 79VA10 provides record access and contesting procedures: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

Formal redress is provided.

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: If inaccurate information is obtained and input into VistA a patient may not know the established process to correct their information

Mitigation: VEText does not maintain patient health records outside of VistA. Patients can easily opt out of the system by replying to a text message with "stop". The patient may also be opted out by VA staff with access to the portal interface. VEText obtains data from VistA. Incorrect information is corrected in VistA using established processes.

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.

There are currently seven levels of access to the VEText Portal (the web interface used to access various functions of the VEText system). All seven levels of access require that the user has an active VistA account and a VA PIV card and PIN for Two Factor Authentication (2FA) through VA SSO. ADMIN and VISN access must be requested by the existing Facility or VISN POC.

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?

Any hospitalist with access to VistA can access VEText at the most basic permission level "All Users." Elevated access is only permitted through additional training and permission from each site's POC. The veteran has the choice to receive information including PII. If it is declined, PII is excluded from appointment reminders.

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.

User Types : All Users - Read-only access to Appointments Tab and Tools Tab; Reports - Read-only access to Appointments Tab, Tools Tab, and Reports Tab; Surgery Notify - Read-only access to Appointments Tab, Tools Tab, Reports Tab, and Surgery Notifications Tab; Surgery Admin - Read-only access to Appointments Tab, Tools Tab, and Reports Tab. Able to configure surgery message templates and add Surgery Notify users; Manager - Read-only access to Appointments Tab, Tools Tab, Reports Tab, and Surgery Notifications Tab, and Admin Tab, Can activate/deactivate Open Slot Management (OSM) clinics, Can manage COVID-19 clinics and add message requests; Admin - Read-only access to Appointments Tab, Tools Tab, Reports Tab, Admin access to Surgery Notifications Tab and Admin Tab, Can configure all settings, Can add Reports, Manager, Surgery Admin, and Surgery Notify users; VISN - Read-only access to Appointments Tab, Tools Tab, Reports Tab, Admin access to Surgery Notifications Tab and Admin Tab, Can configure all settings, Can add Reports, Manager, Surgery Admin, and Surgery Notify users, Can view VISN level reports.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Contractors will have access to the system and the PII/PHI only if their role requires access as part of their required duties. Contractors may be involved in the design and development of future enhancements and/or maintenance and support of the system. All contractors accessing the system are required to follow VA policies and procedures to obtain and maintain a VA Network account before accessing the VEText Assessing system. The Contracting Officer Representative (COR) verifies contractor eligibility for VA network access including a favorable background investigation, signed NDA, and annual VA privacy training. If access to CDW PII and PHI data is required, contractors will be required to complete the National Data Services (NDS) ePAS User Request process.

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.

Users are required annually to complete "VA Privacy and Information Security Awareness and Rules of Behavior" and "VA Privacy and HIPAA Training."

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* July 30th, 2021
3. *The Authorization Status:* ATO is Current
4. *The Authorization Date:* October 7th, 2021
5. *The Authorization Termination Date:* October 6th, 2024
6. *The Risk Review Completion Date:* September 13th, 2021
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.***

ATO process has been completed.

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)*

No, the system does not use cloud technology.

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 VEText is not utilizing any Cloud Service Provider

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. VEText is not utilizing any Cloud Service Provider.

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. VEText is not utilizing any Cloud Service Provider.

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. VEText is not utilizing any Robotics Process Automation.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.08.23 13:02:50 -04'00'

Privacy Officer, Nancy Katz-Johnson

RANDALL SMITH

Digitally signed by RANDALL SMITH
Date: 2023.08.23 09:43:23 -05'00'

Information System Security Officer, Randall Smith

SHANE ELLIOTT

Digitally signed by SHANE ELLIOTT
Date: 2023.08.23 08:58:18 -07'00'

Information System Owner, Shane Elliott

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).

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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