Privacy Impact Assessment for the VA IT System called:

VEText

Office of the CTO

Date PIA submitted for review:
May 7, 2021

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Nancy Katz-Johnson</td>
<td><a href="mailto:Nancy.katz-johnson@va.gov">Nancy.katz-johnson@va.gov</a></td>
<td>203-535-7280</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Roland Parten</td>
<td><a href="mailto:Roland.parten@va.gov">Roland.parten@va.gov</a></td>
<td>205-534-6179</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Robert Durkin</td>
<td><a href="mailto:Robert.durkin@va.gov">Robert.durkin@va.gov</a></td>
<td>909-801-5611</td>
</tr>
</tbody>
</table>
Abstract

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

VEText is a VA-developed appointment reminder system that pulls appointment data from VistA and sends an appointment reminder text message [via third party Short Message Service (SMS) gateway] 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 also 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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PHI is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? 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.
• Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

VEText uses a third-party telecommunications gateway service called Twilio to securely send and receive Short Message Service (SMS) text messages to/from patients. If the Veteran’s response is to cancel, the VEText software cancels the appointment in VistA. This service provides convenience to Veterans and increases VA operational efficiency 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 commercial medical community.

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 was developed wholly by the VA and is hosted and maintained on servers internal to the VA network. VEText uses 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).

Twilio is a cloud-communications service that allows software developers to programmatically send and receive SMS text messages using its web service Application Programming Interface (API). VEText uses an HTTP Secure Sockets Layer (SSL) connection to securely send SMS messages to patients through the Twilio service and to receive SMS responses from patients. Twilio generates a URL web hook for the Veteran to click to confirm or cancel the appointment.
Amazon Web Services (AWS) is a commercial cloud service provider. A Virtual Machine in the AWS cloud is used as the endpoint for the URL sent via text message. This enables the Veteran to cancel the appointment since both AWS and the Veteran are located outside of the VA firewall. VA developed the software script used to listen for the response. 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. This capability was included in the Authority to Operate (ATO) and a Plan of Action and Milestones (POA&M). The business owner for VEText is Chris Johnston from the Office of the CTO.

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 (MSSQ) 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 via the Twilio service, but Twilio does not store any PHI/PII on their system due to phone number and message body redaction.

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 Number (SSN).

**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://vaow.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.*

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**
PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>No</td>
<td>No</td>
<td>Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status</td>
<td>For sending messages and reporting.</td>
<td>Username, password, various levels of access, SSL encryption for transmission.</td>
</tr>
<tr>
<td>MSSQL Server Database</td>
<td>Yes</td>
<td>Yes</td>
<td>Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status</td>
<td>For sending messages and reporting.</td>
<td>Username, password, various levels of access, SSL encryption for transmission.</td>
</tr>
</tbody>
</table>
### 1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Patient name, ICN, phone number, appointment date and time, and clinic name come directly from VistA, which is the only source of scheduled appointments for patients.

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 VEText SMS indicates a vaccination outside of the VA. VEText also records responses of PASS indicating the patient is not interested in the vaccine with the VA.

### 1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

<table>
<thead>
<tr>
<th>Source</th>
<th>Direct</th>
<th>From Other Sources</th>
<th>Source of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MongoDB Database</td>
<td>Yes</td>
<td>Yes</td>
<td>SSL encryption for transmission.</td>
</tr>
<tr>
<td>Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status</td>
<td>For sending messages and reporting.</td>
<td>Username, password, various levels of access, SSL encryption for transmission.</td>
<td></td>
</tr>
</tbody>
</table>
another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Patient name, ICN, phone number, appointment date and time, last four of SSN, and clinic name come directly from VistA via standard Remote Procedure Calls (RPCs). COVID-19 vaccination status and interest are collected from the CDW or directly from the patient.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This question is related to privacy control AP-2, Purpose Specification.

VEText (Text Message Appointment Reminders) is an SMS communication system written by VA staff that pulls appointment data from VistA and sends an appointment reminders or notifications (via third party SMS gateway) to Veterans allowing them to either schedule, confirm, or cancel appointments. VEText uses the following PII:

- Name
- Phone Number
- Appointment Date/Time
- Clinic Name
- Last four SSN
- COVID-19 Vaccination Interest/Status

Without the phone number, VEText would not be able to send the message to the patient. Appointment Date/Time and Clinic Name are used in the content of the message to remind the Veteran of their appointment. Name is used in reporting to internal staff to identify Veterans that may need their appointment re-scheduled. SSN is used for matching patient data and reporting. COVID-19 Vaccination Interest/Status is used for reporting and targeting COVID-19 vaccination messaging.

1.5 How will the information be checked for accuracy? How often will it be checked?
Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

VEText retrieves the 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.

1.6 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), 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:

- System of Record Notice - 79VA10 Veterans Health Information Systems and Technology Architecture-VA

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.
Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

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

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

**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:**
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.
   
   **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.

**2.2 What types of tools are used to analyze data and what type of data may be produced?**
Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

VEText does not make any information available to the users of the system that is not already available in the Electronic Health Record (VistA).

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

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

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

**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**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.

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. The system owner is responsible for ensuring these 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

The following information is retained in VEText:
- Name
- Phone Number
- VistA ICN
- Appointment Date/Time
- Clinic Name
- Last four of SSN
- COVID-19 Vaccine Interest/Status

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

Data is retained in the short-term (up to 14 days) for the purpose of processing confirm or cancel requests from veterans. The software matches the response from the veteran with the appointment that has been cached by the system. Longer-term storage of the data (up to one year) is for the purposes of reports, statistics, and other system metrics.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.
An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

The retention schedule applicable to VEText is GRS 5.2 Transitory and Intermediary Records https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

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.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

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:** Data retained longer than necessary could be at risk to be released inadvertently.

**Mitigation:** VEText follows the retention schedule listed in 3.2 and that data is retained in the short-term (up to 14 days) for the purpose of processing confirm or cancel requests from veterans and longer-term storage of the data (up to one year) is for the purposes of reports, statistics, and other system metrics. Data is stored only as necessary and then purged. Data is stored on secured servers and is encrypted. The system retains data only so long as is necessary to perform its tasks, such as processing responses received from veterans (e.g. cancel an appointment) and for reporting purposes. The privacy risk is low in that the data is temporarily stored and is stored on servers that are secured. Data is accessed only by authorized individuals.

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

*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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VistA</td>
<td>VEText gathers necessary information from VistA to send pertinent text messages.</td>
<td>Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN</td>
<td>Remote Procedure Calls (RPC)</td>
</tr>
<tr>
<td>CDW</td>
<td>VEText stores application configuration information and caches some VistA information.</td>
<td>Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status</td>
<td>Extract Transform Load (ETL)</td>
</tr>
</tbody>
</table>

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

Follow the format below:

**Privacy Risk:**
Sensitive information may be accessed by un-authorized individuals

**Mitigation:**
Access to the information is controlled by an approval process to provide the level of access required that limits the access to only the VistA instance and Medical Center Electronic Health Record (VistA) the user is authorized to access. Thus, each user can only see the information for their particular site that they were previously authorized for. 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. Access to the VEText portal is controlled by VistA access and VA Single Sign-on Internal (SSOi). VEText portal log in information is logged. The system owner is responsible for ensuring these safeguards are in place and functioning.
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: This question is #7 in the Privacy Threshold Analysis.

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

<table>
<thead>
<tr>
<th>Program Office or IT System</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twilio</td>
<td>Receiving from VEText and transmitting to cell phones.</td>
<td>First Name, Appointment Date/Time, Clinic Name, Cell Phone Number, COVID-19 Vaccination Interest/Status</td>
<td>Routine Use #29 – 24VA10A7</td>
<td>SSL HTTP Post</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Not applicable

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:**
Sharing information externally may result in information being accessed by unauthorized individuals.

**Mitigation:**
VEText shares the minimal information necessary with the external SMS Gateway (Twilio) to access and send SMS messages to Veterans Cell Phones. VEText 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. The VEText application connects with the SMS Gateway via SSL and authenticates with an ID and security key. All data is encrypted with this ID and Key and then transmitted to the SMS Gateway to send to Veterans. The SMS gateway does not store the cell phone number or the content of the message as the VA has purchased and implemented phone number redaction and message body redaction services.

### Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Veterans are notified of data collection and privacy policy’s upon registration with Veterans Health Information Systems and Technology Architecture (VistA) Records-VA and is available in SORN 79VA10.  

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. 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.

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.

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:**
If an individual is not given proper notice, they may be giving up information that they do not want to be used

**Mitigation:**

1. **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. Individuals are provided notice upon VHA registration as well as in the Notice of Privacy Practices as seen in the Appendix.

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.

2. **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.

3. **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 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

**7.1 What are the procedures that allow individuals to gain access to their information?**

*Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.*

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

*If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*
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 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 for VA and has an established process for release of information to obtain a copy of or make changes to information in VistA.

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. Therefore, there would be no inaccurate or erroneous information to correct.

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

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

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.
The system does not maintain health records outside of VistA. Therefore, there would be no inaccurate or erroneous information to correct.

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.

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?

Describe the process by which an individual receives access to the system.
Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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.

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 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 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?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).
Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your Initial Operating Capability (IOC) date.

1. 10/22/2018
2. Full ATO
3. 3 Years
4. Moderate
### Section 9. References

**Summary of Privacy Controls by Family**

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

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

Nancy E Katz-Johnson 206244
Digitally signed by Nancy E Katz-Johnson 206244
Date: 2021.06.09 09:50:56 -04'00'
Privacy Officer, Nancy Katz-Johnson

Roland B Parten 596219
Digitally signed by Roland B Parten 596219
Date: 2021.06.09 09:09:42 -05'00'
Information Systems Security Officer, Roland Parten

Robert M Durkin 121091
Digitally signed by Robert M Durkin 121091
Date: 2021.06.09 10:19:17 -04'00'
System Owner, Robert Durkin
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).