Privacy Impact Assessment for the VA IT System called:

Check-in Experience

VACO

VHA – Office of Veteran Access to Care

Date PIA submitted for review:

May 26th, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	(202) 632 – 8423
Information System Security Officer (ISSO)	Karen McQuaid	karen.mcquaid@va.gov	(708) 724 – 2761
Information System Owner	Christopher Johnston	christopher.johnston2@va.gov	(202) 503 – 6267

Abstract

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

The Check-in Experience (CIE) IT systems provides VHA patients the ability to check in for scheduled health appointments and conduct check-in related activities from personal mobile devices. CIE utilizes a combination of existing systems, including VEText, VA.gov, VistA, and VA Profile and new subsystems to deliver this functionality. These new sub-systems are:

(1) Check-in Integration Point (CHIP), which is a new back end subsystem that interfaces with VistA, VA.gov, VA Profile, and other VA-controlled systems to gather appointment and patient related information and process patient check in activities;

(2) Low Risk One Time Authentication/Authorization (LoROTA), which is a new back end subsystem that enables patients to access a limited set of low risk information about their appointment and patient profile upon establishing their identity through use of device- and secrets based factors.

These two new subsystems are part of the larger CIE system. The larger CIE system overlaps with existing authorized systems, such as VA.gov and VEText. The scope of this Privacy Impact Assessment (PIA) is to cover all aspects of the CIE system.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

- *A. The IT system name and the name of the program office that owns the IT system.*
- *B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *C. Indicate the ownership or control of the IT system or project.*

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.*
- *E. A general description of the information in the IT system and the purpose for collecting this information.*
- *F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*

3. Legal Authority and SORN

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

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

D. System Changes

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

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

Check In Experience (CIE) is a new IT system owned by VHA Office of Veteran Access to Care (OVAC). The business purpose of CIE is to provide VHA patients the ability to check in for scheduled health appointments and conduct check-in related activities from personal mobile devices. This increases appointment compliance and patient satisfaction. The IT system is owned and controlled by the Office of the Chief Technology Officer within the Office of Information and Technology.

There are roughly 9 million scheduled outpatient appointments per month within the VHA system. It is expected that CIE will be utilized for a fraction of those appointments to complete pre-appointment and/or day-of check-in activities. Best estimates at this time are 5% of appointments, or roughly 450,000 appointments per month. Since VHA patients typically have multiple appointments, we expect the total number of individuals with information stored in the system to be less than 450,000. A typical affected individual is an existing VHA patient with a scheduled outpatient appointment at a VHA facility with a VHA provider. This individual would utilize CIE to complete pre-appointment activities before arriving at a VHA facility, and then utilize CIE to complete check-in after arrival at a VHA facility.

Initially CIE will handle and process basic information related to upcoming appointments that is already stored in other VA systems. For example, information about when and where a particular patient may have appointments on a given day. In addition, CIE will initially temporarily store inputs from patients using CIE, including a date/time stamp of when a patient completed on-site check-in and confirmation that certain demographic information is correct. After initial launch, it is expected that CIE will temporarily store additional inputs from patients using CIE, including updates to address, telephone, emergency contact and next of kin information. In all instances, CIE will not serve as a final or canonical data store for any information. Instead, CIE functions as an integration point where data is moved between systems and users, and then stored in systems that are outside CIE. For example, when a patient completes check-in via CIE for a specific outpatient appointment, the resulting check-in information is stored within a VistA system after passing through CIE.

Information collected by CIE will be shared with individual VistA EHR instances. Primarily this information will be confirmation that demographic information is correct and date/time stamp of check in for scheduled appointments. As noted above, after initial launch, it is expected that CIE will share additional inputs from patients.

CIE is a national system that is centrally maintained and available to all VHA health care facilities for assisting with scheduled appointment check-in and appointment preparation activities. CIE is run as a singular instance, therefore maintaining PII consistency across multiple instances is not applicable.

The legal authority to operate this IT System is 38 U.S. Code § 7301, which establishes the Veterans Health Administration within the Department of Veterans Affairs to, "provide a complete medical and hospital service for the medical care and treatment of veterans." Establishment of systems that allow patients to check-in and prepare for their medical appointments is a necessary part of providing this service.

Because CIE presents new functionality, it is expected that VHA facilities utilizing CIE for scheduled appointment check-in and appointment preparation activities may alter related business processes on a facility or individual clinic level. If it is determined during the course of completing this PIA that additional privacy concerns must be addressed and a technology change is the most effective way of addressing those concerns, then technology changes will be made.

Modification of SORN is not applicable.

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)

Other unique identifying information:
• Patient Data File Number (DFN) • Patient Internal Entry Number (IEN) • Cell phone number

PII Mapping of Components (Servers/Database)

CIE consists of two key components that persist data for a short period before passing data on to an end user or canonical data store. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CIE 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
LoROTA DB	No	Yes	• Name • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc., of a different individual) • Integration Control Number (ICN) • Next of Kin • Patient DFN • Patient IEN • Clinic Name	Identity verification, one-time authorization, and confirmation of data	Access to production data is granted only to holders of a specific JavaScript Web Token (JWT), which is only provided to authorized systems. Data is encrypted in transit and is permanently removed from the database within 24 hours of instantiation. All logging functions are designed to eliminate the accidental collection of PII in logs.

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?

Data used by CIE systems originates from VHA's VistA EHR system. CIE also makes use of end-user cellphone numbers and device IP addresses to complete appointment check-in or appointment preparation activities

VistA EHR system source information includes Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Integration Control Number (ICN), Next of Kin, Patient DFN, Patient IEN, Cell Phone Number and Clinic Name.

Data collected from an individual includes Internet Protocol (IP) Address Numbers and Cell phone Number.

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.

CIE utilizes data provided by VistA (a VA system) to retrieve patient appointment data and provide it to the patient. No data is taken from commercial sources.

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

N/A

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?

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.

Data	**Collection Method**
Name	Electronic transmission

Personal mailing address	Electronic transmission
Personal phone number(s)	Electronic transmission
Personal email address	Electronic transmission
Emergency contact information (name, phone number, etc., of a different individual)	Electronic transmission
Internet Protocol (IP) address numbers	Automatically provided by individual when accessing CIE
Integration Control Number (ICN)	Electronic transmission
Next of kin	Electronic transmission
Patient DFN	Electronic transmission
Patient IEN	Electronic transmission
Clinic name	Electronic transmission
Cell phone number	Automatically provided by individual when accessing CIE
Date of Birth	Electronic transmission

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.

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.

Cell phone number data supplied by the individual is checked against existing telephone records in the VistA EHR for accuracy. All other information temporarily stored by CIE is not checked for accuracy as CIE does not serve as the canonical store for that information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

38 U.S. Code § 7301, which establishes the Veterans Health Administration within the Department of Veterans Affairs to, "provide a complete medical and hospital service for the medical care and treatment of veterans." Establishment of systems that allow patients to check-in and prepare for their medical appointments is a necessary part of providing this service. The CIE system has been approved as the System of Records to execute the identity verification and authorization detailed in 24VA10A7 - Patient Medical Records – VA.

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: Unintended disclosure of PHI/PII via unauthorized system access to system data/applications.

Mitigation: Using tightly controlled system access and numerous enterprise and system level cybersecurity measures in place to prevent unauthorized access; data only temporarily retained to reduce potential scale of unintentional disclosure. Logs are configured to not store any PII/PHI to avoid duplication.

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.

- Name: Presented to user to verify accuracy and completeness; last name used by CIE as part of identity verification
- Date of Birth: Presented to user to verify accuracy and completeness; DoB used by CIE as part of identity verification
- Personal Mailing Address: Presented to user to verify accuracy and completeness
- Personal Phone Numbers(s): Presented to user to verify accuracy and completeness
- Personal Email Address: Presented to user to verify accuracy and completeness
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): Presented to user to verify accuracy and completeness
- Internet Protocol (IP) Address Numbers: Collected as part of HTTP/S protocol and logging system
- Integration Control Number (ICN): Utilized for system-to-system identification of records
- Next of Kin: Presented to user to verify accuracy and completeness
- Patient DFN: Utilized for system-to-system identification of records
- Patient IEN: Utilized for system-to-system identification of records
- Clinic Name: Presented to the user during the check in process
- Cell Phone Number: Collected and used by CIE as part of identity verification

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.

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.

No additional analysis is undertaken with data utilized by CIE. New data created by CIE consists of date/time stamps of appointment check in and appointment related transactions, which is temporarily stored by CIE and transmitted to other systems for permanent storage.

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?

All data is encrypted in transit via the Transit Layer Security protocol (TCP/TLS) over port 443. Data temporarily stored with CIE data stores is accessible only with holders of an authorized JavaScript Web Token (JWT). Access to JWTs is tightly restricted to authorized systems. In addition, data is removed from the LoROTA datastore within 24 hours. In addition, data stored in LoROTA data stores is encrypted at rest.

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

CIE does not utilize, request, or record new SSNs. The ICN is used by downstream systems as an identifier and not presented to patients. Patients provide their DOBs and names for verification. All data is encrypted at rest and in transit.

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

PII/PHI is safeguarded in accordance with OMB Memorandum M-06-15 by engaging in and completing the Privacy Threshold Assessment and Privacy Impact Assessment processes in collaboration with the VA's Senior Agency Official for Privacy.

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?

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

2.4c Does access require manager approval?

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

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

VAEC maintains logs of administrative accounts accessing the information system and databases. Datadog is installed on the servers and sends logs based on thresholds set by development team. The development team has configured Datadog to report on administrative account usage.

The Contracting Officer Representative (COR) is required to approve elevated privilege requests that allow users to gain administrative access to the information systems and databases.

Use of information by CIE is tightly scoped to the purpose of the CIE system: to assist VHA patients in preparing for and checking into their scheduled health care appointments. Only data that is necessary to complete CIE transactions is retrieved from other VA systems or collected by individuals. Once data is retrieved or collected, it is either destroyed within 30 days (and in many cases, 24 hours) or transmitted to another authorized system and then destroyed. All persons with administrative access to CIE are required to undergo annual privacy and security training and are subject to the requirements and disciplinary actions set forth in VA Handbook 6500. Administrative access, which includes access to system components where sensitive information is processed or stored, is tightly controlled and each access event is recorded.

AWS GovCloud provides the infrastructure to protect PII when stored or in transit, and VAEC has enabled controls and processes to ensure that there are safeguards around PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The following data is retained temporarily for processing use and then destroyed or transmitted to another authorized system with its own retention policy and then destroyed:

- Name

- Date of Birth
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Internet Protocol (IP) Address Numbers
- Integration Control Number (ICN)
- Next of Kin
- Patient DFN
- Patient IEN
- Clinic Name
- Cell Phone Number

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.*

- Name: 24 hours*
- Date of Birth: 24 hours*
- Personal Mailing Address: 24 hours*
- Personal Phone Number(s): 24 hours*
- Personal Email Address: 24 hours*
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): 24 hours*
- Internet Protocol (IP) Address Numbers: 30 days*
- Integration Control Number (ICN): 30 days*
- Next of Kin: 24 hours*
- Patient DFN: 30 days*
- Patient IEN: 30 days*
- Clinic Name: 24 hours*
- Cell Phone Number: 24 hours*

Note: LoROTA backups are retained for 35 days. LoROTA Data backups occur at minimum every 5 minutes and at least once every 24 hours. Appointment data (including patient demographic data) is kept from the time of retrieval (after the appointment has been entered into VistA) until the appointment date has passed. Data is checked every 24 hours to see if appointment dates have passed. Data related to past appointments is removed from LoROTA database every 24 hours.

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

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

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

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

No retention schedule specifically for CIE has been approved by the VA records office and the National Archives and Records Administration. However, CIE does not serve as the destination for any data. Instead, CIE acts as an intermediary data process and system integration point and relies on systems to which it is connected to maintain approved retention schedules.

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.

At the end of each retention period, a data clean-up job is executed automatically to permanently delete all expired data. In the event data is ever stored to removable magnetic storage media, that media is wiped and sent out for destruction per VA Handbook 6500. Any digital media is shredded or sent out for destruction per VA Handbook 6500.

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.

All protections discussed in this PIA are applied to CIE research, testing, and training environments.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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: Any data temporarily stored by CIE is at risk for unintended disclosure via unauthorized system access.

Mitigation: CIE retains data for the minimum amount of time necessary to support the system's objective. Retention policies are regularly re-evaluated to determine whether shorter retention periods may be advisable to further protect privacy.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VistA (received from)	For identity verification and authorization; for review of contact and other demographic information as part of the appointment preparation and check-in process; for tracking patient data across systems	Name Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Emergency Contact Information (Name, Phone Number, etc. of a different individual) Integration Control Number (ICN) Next of Kin Clinic Name Patient DFN Patient IEN	Electronic transmission via secure protocol
Vets.gov/VA.gov (shared with)	For identity verification and authorization; for review of contact and other demographic information as part of the appointment preparation and check-in process; for tracking patient data across systems	Name Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Emergency Contact Information (Name, Phone Number, etc. of a different individual) Integration Control Number (ICN) Next of Kin Clinic Name	Electronic transmission via secure protocol

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*
		Patient DFN Patient IEN	
Telehealth and Scheduling Portfolio - Clinician Workflow API	Provide interface to retrieve Veteran Appointment information and VistA Clinic information to support the VSECS Staff Application	Patient DFN Patient IEN Integration Control Number (ICN) Clinic name Appointment data	API

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: Any data shared within the Department by CIE is at risk for unintended disclosure via unauthorized system access.

Mitigation: All data is encrypted in transit via the Transit Layer Security protocol (TCP/TLS) over port 443. Access to the means of transmission is controlled through the use of authorized JavaScript Web Tokens (JWTs). Access to JWTs is tightly restricted to authorized systems. In addition, data is removed from the LoROTA datastore within 24 hours. All persons with administrative access to CIE are required to undergo annual privacy and security training and are subject to the requirements and disciplinary actions set forth in VA Handbook 6500. Administrative access, which includes access to system components where sensitive information is processed or stored, is tightly controlled and each access event is recorded.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
n/a	n/a	n/a	n/a	n/a

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: No data is shared with external organizations.

Mitigation: Not applicable.

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.

Yes, the VA.gov privacy notice is presented to individuals utilizing systems connected to CIE and accessible at https://www.va.gov/privacy-policy/#on-this-page-76

24VA10A7 - Patient Medical Records – VA

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

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

The privacy policy is utilized throughout VA and applicable to CIE as a system. Privacy requests are carried out by VA rather than CIE directly.

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

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

Yes, individuals may decline to utilize the mobile check-in process and instead proceed to a clerk or seek other means to check into scheduled health care appointments.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Individuals consent to the particular uses of information by CIE by accessing systems connected to CIE and engaging in the mobile check in process.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> 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: Consent for CIE to process information may not be sufficiently clear to individuals engaging with systems connected to CIE.

Mitigation: Additional investigation of digital consent models on VA.gov will be conducted to identity any additional means of providing further opportunity to consent

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.***

Individuals may gain access to information processed by CIE via VA's established Freedom of Information Act process. In addition, certain information processed by CIE may also be available under the provisions of the Health Insurance Portability and Accountability Act.

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

N/A

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

N/A

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Any inaccurate or erroneous information identified by an individual may be corrected by an authorized member of VHA administrative or clinical staff, including Medical Services Assistants (MSAs) and scheduling clerks. **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.

Systems connected to CIE instruct individuals utilizing CIE for appointment check-in or preparation for an appointment to speak with a VHA staff member to correct any inaccurate or erroneous information.

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.

In addition to correcting information per the procedures discussed above, future CIE capability may allow individuals to update information directly via systems connected to CIE.

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: No identifiable risk as CIE does not store veterans' data.

Mitigation: Not applicable.

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.

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?

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.

Access control for the following user types is detailed below:

VHA Patient (end user)
VHA patients (end users) do not directly access CIE. Instead, VHA patients access CIE via a combination of Short Messaging Service (SMS) messages and interaction with web pages hosted on VA.gov. In order to gain access to CIE via SMS and VA.gov, VHA patients must: (1) utilize a physical device that is addressed with a telephone number that matches a phone number listed in their VistA EHR patient profile; (2) provide information that only they should know about themselves. This two-step procedure of utilizing "something you have" and "something you know" provides two factors of identity security around access to CIE via SMS and VA.gov.

VHA staff member (end user)
VHA staff members, including administrative and clinical staff do not directly access CIE. Instead, VHA staff members interact with one of two tools which is connected to CIE: (1) VistA Scheduling Enhancements Graphical User Interface (VSE GUI); or (2) VistA Scheduling for Clinical (VSE for Clinical) web application. Access to both tools is controlled via VA's centrally managed Single Sign On Internal (SSOi) program.

Developer/administrator
Developers and administrators are authorized to interact directly with CIE for official purposes. These include developing and deploying new features, monitoring system performance, analyzing unexpected behavior or performance degradations, audit purposes, and other purposes necessary to ensure CIE delivers its business objectives. Access is controlled via VA Enterprise Cloud (VAEC) identity and access management (IAM) policies and configuration, which relies in part on VA's centrally maintained active directory. In addition, developers and administrators can access CIE programmatically via Amazon Web Services (AWS) System Manager (SSM) service pursuant to VAEC governance requirements.

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.

Yes, VA contractors have access to CIE and PII processed by CIE and are directly involved in the development, operations, and maintenance of CIE. Before gaining developer/administrator access to CIE as detailed above, VA contractors must complete required security and privacy

trainings and commit to adherence of the policies established in VA Handbook 6500. In addition, VA contractors sign the Contractor Rules of Behavior and complete a Nondisclosure Agreement.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All developer/administrators with access to CIE complete VA required privacy and security training on an annual basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* May 4th, 2022
3. *The Authorization Status:* Authorized for 180 days
4. *The Authorization Date:* May 25th, 2023
5. *The Authorization Termination Date:* December, 2023
6. *The Risk Review Completion Date:* May 25th, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, CIE uses Amazon Web Services (AWS) cloud technology within the US GovCloud regions, which has FedRAMP authorization. Usage of AWS by CIE is provisioned through the VA Enterprise Cloud (VAEC) program under an Infrastructure-as-a-Service model. CIE is a Platform-as-a-Service and leverages the serverless technology and security functionality provided by VAEC.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of*

the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Not applicable, CIE uses VAEC.

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.

Not applicable, CIE uses VAEC.

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.

Not applicable, CIE uses VAEC.

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

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

Not applicable, CIE uses VAEC.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Tonya L.
Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.07.06 11:28:23 -04'00'

Privacy Officer, Tonya Facemire

Karen A.
McQuaid 321576

Digitally signed by Karen A. McQuaid 321576
Date: 2023.07.05 09:19:34 -05'00'

Information System Security Officer, Karen McQuaid

Digitally signed by CHRISTOPHER JOHNSTON
Date: 2023.07.07 18:03:53 -04'00'

Information System Owner, Christopher Johnston

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

VA Privacy Policy : https://www.va.gov/privacy-policy/#on-this-page-76

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

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