



Privacy Impact Assessment for the VA IT System called:

**Get Well Network (GWN)**  
**Veterans Health Administration**  
**Infrastructure Operations**  
**eMASS ID #2572**

Date PIA submitted for review:

1/7/2025

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	(503) 721-1037
Information System Security Officer (ISSO)	Roland Parten	Roland.Parten@va.gov	(205) 534-6179
Information System Owner	Gail Nemetz	Gail.Nemetz@va.gov	(216) 849-6020

## Abstract

*The abstract provides the simplest explanation for “what does the system do for VA?”.*

Get Well Network (GWN) interactive patient care information system provides education, information, entertainment, and access to the internet for inpatient veterans. The Get Well Network (GWN) Government Interface Servers (GIS), which are host at Cleveland Data Center, provide the interface between the Get Well Network (GWN) bedside application the VA Electronic Health Care Record (VistA) and Computrition Meal Ordering. This application receives PII/PHI from the VistA Electronic Health Record and is primarily used by inpatient ward nurses and the inpatient veterans at multiple VA Medical Centers.

## Overview

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

### *1 General Description*

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

Get Well Network (GWN) is used by VA to provide educational, information, entertainment, and access to the internet for inpatient veterans. Get Well Network (GWN) Government Interface Service (GIS) provide the interface between the Get Well Network (GWN) bedside application, Computrition Hospitality Suite, Oracle Database, and the VA Electronic Health Care Record (VistA). This application receives PII/PHI from the VistA Electronic Health Record via Health Level 7 (HL7) and is primarily used by inpatient ward nurses and the inpatient veterans.

- B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

### Infrastructure Operations

### *2. Information Collection and Sharing*

- C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

Get Well Network (GWN) application is used at VHA licensed medical centers clinical and administrative personnel (4001+) which includes healthcare providers and inpatient veterans or dependents.

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input type="checkbox"/>	Clinical Trainees
<input type="checkbox"/>	VA Contractors
<input type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

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

The purpose of Get Well Network is to help patients take an active role in their health care, operationalize the Whole Health Model of Care and improve quality, patient satisfaction, and clinical workflow/operations through patient engagement in the inpatient/long term care setting.

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

The Get Well Network (GWN) Government Interface Service (GIS) connects a Get Well’s Patient Life System (PLS) server with the VistA/CPRS system for a VA medical facility. The function of GIS is to receive inbound Health Level 7 (HL7) data feeds from VistA/CPRS and obfuscates PHI using transformation rules before transmitting the messages over the VA firewall crossing the internet. The messages traverse the Get Well firewall where they are received by Get Well’s Patient Life System (PLS) server, Inpatient Module. GIS receives outbound data feeds from the Get Well’s Patient Life System (PLS) server, Inpatient Module and re-inserts the corresponding PHI values by reversing the transformations before transmitting it to the facility VistA/CPRS.

In addition to the inbound and outbound data feeds, GIS receives REST Web Service calls from the meal ordering application in the Get Well’s Inpatient Module, re-identifies them and transmits them to Computrition Meal Ordering application (third-party meal ordering service). In the reverse direction, GIS receives REST Web Service calls containing dietary menu updates from the third-party meal ordering system and transmits these

updates to the meal ordering application in the Get Well's Patient Life System (PLS) server, Inpatient Module.

An Oracle database consists of tables that support the transformation of an inbound Health Level 7 (HL7) message sent from VistA/CPRS from one that contains PHI to one that does not contain PHI for use by the Get Well Inpatient Module. In the reverse direction, the database supports the transformation of outbound HL7 messages from the Inpatient Application Server by re-inserting PHI information on messages to VistA/CPRS.

The Get Well Inpatient menus in VistA/CPRS used by care providers to order medication or health education may be updated by Health Level 7 (HL7) messages passed from the Get Well's Patient Life System (PLS) server, Inpatient Module through GIS. To support GIS troubleshooting, the application regularly sends a HL7 heartbeat message to the Get Well's Inpatient Module that Get Well monitors to ensure connectivity.

Information shared by IT system: Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity.

F. Are the modules/subsystems only applicable if information is shared?

Yes.

G. *Is the system operated in more than one site to include primary and secondary 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?*

All Government Interface Servers (GIS) and Oracle Databases are located at Infrastructure Operations Cleveland data centers located Cleveland, Ohio.

### 3. *Legal Authority and System of Record Notices (SORN)*

H. *What is the citation of the legal authority?*

The authority for this interconnection is based on:

- Federal Information Security Modernization Act (FISMA)
- NIST 800-47 Rev 1 Managing the Security of Information Exchanges
- VA Directive and Handbook 6513, Secure External Connections
- VA Directive 6500, VA Cybersecurity Program
- VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security

Version date: October 1, 2024

**Page 4 of 39**

- OMB Circular A-130, Managing Information as a Strategic Resource
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

The authority for the VA to share data for the purpose outlined under Agreement with Get Well is as follows:

- HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- VA Claims Confidentiality Statute, 38 U.S.C § 5701
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332

Get Well Network (GWN)'s legal authorities for operating the system are found in the:

- VA Directive 6500, Managing Information Security, VA Information Security Program, and VA Information Security Program
- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R Part 160
- 38 United States Code (U.S.C.) 5721-5728, Veteran's Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Managing Information as Strategic Resource
- Veterans Health Information Systems and Technology Architecture (VistA) Records

#### *I. What is the SORN?*

Get Well Network (GWN)'s SORNS that apply to the system:

- Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).
- Patient Medical Record – VA, SORN 24VA10A7 <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

*J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

This system is not in the process of being modified nor is it using cloud technology.

#### 4. System Changes

K. Will the business processes change due to the information collection and sharing?

Yes

No

if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

Yes

No

if yes, <<ADD ANSWER HERE>>

## 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 Information collected, used, disseminated, created, or maintained in the system.

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

Name

Full Social Security Number

Partial Social Security Number

Date of Birth

Mother's Maiden Name

Personal Mailing Address

Personal Phone Number(s)

Personal Fax Number

Personal Email Address

- |   |   |  |
|---|---|--|
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a Different Individual) | <input type="checkbox"/> Address Numbers                            | <input type="checkbox"/> Next of Kin   |
| <input type="checkbox"/> Financial Information  | <input checked="" type="checkbox"/> Medications                     | <input type="checkbox"/> Date of Death   |
| <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers Account Numbers                    | <input checked="" type="checkbox"/> Medical Records                 | <input type="checkbox"/> Business Email Address                                  |
| <input type="checkbox"/> Certificate/License Numbers <sup>1</sup>   | <input checked="" type="checkbox"/> Race/Ethnicity                  | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Vehicle License Plate Number   | <input type="checkbox"/> Tax Identification Number                  | <input checked="" type="checkbox"/> Other Data Elements (List Below)             |
| <input type="checkbox"/> Internet Protocol (IP)   | <input checked="" type="checkbox"/> Medical Record Number           |  |
|   | <input type="checkbox"/> Gender/Sex                                 |  |
|   | <input checked="" type="checkbox"/> Integrated Control Number (ICN) |  |
|   | <input type="checkbox"/> Military History/Service Connection        |  |

Other PII/PHI data elements: Event Type Code, Message Date Time, Patient ID, Encounter/Visit ID, Assigned Patient Location, Admission Date Time, Set ID – ZNT, Routing Code, Message to Send, & Date/Time of Message.

**1.2 List the sources of the information in the system**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?*

The VistA system functions as the VA electronic health record (EHR) system. The comprehensive database within VistA provides a single source for Veteran patient data and the care and services available to the Veteran patient.

VistA/CPRS and Get Well’s Patient Life System (PLS) server, Inpatient Module exchange information using the Integrated Framework- Kernel Installation and Distribution System (KIDS) interface. Inbound and outbound data feeds between the two systems pass through the Government Interface Service (GIS). This server obfuscates PHI as it is transmitted between systems.

*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.*

The VistA\CPRS system functions as the VA electronic health record (EHR) system. The comprehensive database within VistA provides a single source for Veteran patient data and the care and services available to the Veteran patient.

---

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Vista\CPRS is the primary clinical application in VistA. It is used by VA clinicians and other designated staff to enter, review, and update information about any Veteran patient. Clinicians use CPRS to record the information about a patient encounter, order testing and procedures, prescribe medication and education, and make referrals.

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

Yes.

To facilitate Admit, Discharge, and Transfer (ADT), orders, progress notes (TIU: Text Integration Utilities), and PRN medication administration activity between the VistA/CPRS and Get Well's Patient Life System (PLS) server, Inpatient Module, the two systems exchange information using health the Integrated Framework- Kernel Installation and Distribution System (VistA KIDS) interface. Inbound and outbound data feeds between the two systems pass through the Government Interface Service (GIS). This service, a proxy, obfuscates PHI as it is transmitted between systems.

The installation and configuration of a DSSEB interface (KIDS) creates all logical links, subscribers, orderable items, order menus, Text Integrated Unit (TIU) titles, and the necessary administrative sign-in account in VistA. Care providers use Get Well Inpatient menus to order items such as videos, brochures, and medical content delivered using the Inpatient Module. The menus consist of order menus, order dialogs, and order sets. (An order set consists of multiple order dialogs.)

### **1.3 Methods of information collection**

*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?*

Directly from individual, received via electronic transmission from other systems, and/or also created by the system itself. Other application(s) could receive patient records from third party healthcare providers and requires scanning into the VistA system.

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

Get Well Network (GWN) information is not collected on a form and is not subject to the Paperwork Reduction Act.

### **1.4 Information checks for accuracy, and 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.*

Data inputs into the Veterans Health Information Systems and Technology Architecture (VistA), patient files as well Text Integration Utility (TIU), Computerized Patient Record Search (CPRS). This technology allows doctors and staff to access a patient`s entire medical record and enables them to enter diagnostic findings, treatment plan procedures and patient-specific notes into the patient`s Electronic Health Record. Application users require a VistA account with CPRS/VistA secondary menu option/security key/VistA Person Class Code, etc. to retrieve and store new data.

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

Get Well Network (GWN) does not check for accuracy by accessing a commercial aggregator of information.

**1.5 Identify the specific legal authorities, arrangements, and agreements that 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*

Title 38 United States Code (U.S.C.) §§1701, 1703, 1710(c), 1712, 3104 and Title 38 Code of Federal Regulation (CFR) Chapter 17 authorizes the provision of Veterans medical, nursing home, and domiciliary care and associated record-keeping.

SORN 79VA10 “Veterans Health Information Systems and Technology Architecture (VistA) Records-VA”, <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

SORN 24VA10A7 “Patient Medical Record-VA”, <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

**PRIVACY IMPACT ASSESSMENT: Characterization of the information**

Version date: October 1, 2024

**Page 9 of 39**

*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:* *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization:* *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

*Principle of Individual Participation:* *The program, to the extent possible and practical, collects information directly from the individual.*

*Principle of Data Quality and Integrity:* *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*

*This 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:** The Get Well Network, Government Interface Server (GIS) applications retrieve and collect Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

**Mitigation:** The Department of Veterans Affairs is careful to only collect the information necessary to identify the Veteran in crisis, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the Veterans' information. Users are trained on how to handle sensitive information by taking VA Privacy and Security Awareness Training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

## **Section 2. Uses of the Information**

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

### **2.1 Describe how the information in the system that will be used in support of the program's business purpose.**

*Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.*

PII/PHI Data Element	Internal Use	External Use
Name (Last name, First Name, Middle Initial)	Used as a person's identifier	Not used
SSN	Assists in uniquely identifying the person's medical record.	Not used
Date Of Birth	Assists to identify patient age and confirm patient identity	Not used
Personal Mailing Address	Used to contact the individual	Not used
Personal Phone Number(s)	Used to contact the individual	Not used
Personal e-mail Address	Used to contact the individual	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used to file claims	Not used
Current Medications	Assists to determine medical history and healthcare outcome and used to administer medication	Not used
Previous Medical Records	Assists to determine medical history and healthcare outcome	Not used
Race/Ethnicity	Assists to determine Race/Ethnicity.	Not used
Medical Record Number	Assists in uniquely identifying the person's medical record	Not used
Other Unique Identifying Number (ICN Internal Control Number)	Assists in uniquely identifying the person's medical record	Not used
Date of activity	Used to identify the date/time of visit. Included in the TIU note.	Not used

**2.2 Describe the types of tools 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?*

VA issues guidelines maximizing the objectivity of disseminated Privacy Act information in VA Directive 6502. VA issues guidelines maximizing the objectivity of disseminated Privacy Act

information in VA Directive 0009. VA Privacy Service establishes in VA Directive 6502, p. 7 that: ‘(2) To the greatest extent practicable, the PII is collected directly from the individual to whom it pertains; and ‘(3) When it is not possible to collect PII directly from the individual and that information is collected from third parties, it will be verified with the subject of the record to the greatest extent practicable before any negative action is taken. The VA defines the frequency on which it will check for, and correct as necessary, inaccurate, or outdated PII used by its programs or systems as ‘continuously, and as needed. VA issues guidelines ensuring the quality of disseminated Privacy Act information in VA Directive 0009. VA issues guidelines ensuring the utility of disseminated Privacy Act information in VA Directive 0009. VA issues guidelines maximizing the objectivity of disseminated Privacy Act information in VA Directive 0009.

*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.*

Get Well Network, Government Interface Server (GIS) application do not analyze or produce patient data. This program is designed to provide the interface between the Get Well Network (GWN) bedside application, Computrition Hospitality Suite, Oracle Database, and the VA Electronic Health Care Record (VistA). Get Well Network (GWN) interactive patient care information system provides education, information, entertainment, and access to the internet for inpatient veterans. This application receives PII/PHI from the VistA Electronic Health Record via Health Level 7 (HL7)

### **2.3 How the information in the system is secured.**

*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

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

Data is encrypted when it resides in VistA. Social Security Numbers are often abbreviated to give added protection. The hard drives that the applications/databases are hosted on are encrypted. Applications require specific menus/keys in VistA in order to access the information.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).*

The function of GIS is to receive inbound Health Level 7 (HL7) data feeds from VistA/CPRS and obfuscates PHI using transformation rules before transmitting it to the Get Well's Patient Life System (PLS) server, Inpatient Module. GIS receives outbound data feeds from the Get Well's Inpatient Module and re-inserts the corresponding PHI values by reversing the transformations before transmitting it to the facility VistA/CPRS.

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

Application protection: Only available to approved users.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, is encrypted. SSN are viewable in partial form.

## **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?*

Get Well Network application end users require a Veterans Health Information Systems and Technology Architecture (VistA) account and Active Directory network account; and VistA application-specific VistA menus and/or VistA security keys and may require role-based Active Directory security groups.

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?*

Get Well Network application access is the responsibilities of the applications end users' local site OI&T personnel. Local site OI&T personnel follows their procedures and coordinate access with the applications end users' supervisor.

*2.4c Does access require manager approval?*

Yes. Get Well Network application access requires manager/supervisor approval.

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

Get Well Network (GWN) Government Interface Service (GIS) connects a Get Well's Patient Life System (PLS) server, Inpatient Module (PLS) with the VistA/CPRS system for a VA medical facility. The function of GIS is to receive inbound Health Level 7 (HL7) data feeds from VistA/CPRS and obfuscates PHI using transformation rules before transmitting it to the Get Well's Inpatient Module. GIS receives outbound data feeds from the Get Well's Inpatient Module and re-inserts the corresponding PHI values by reversing the transformations before transmitting it to the facility VistA/CPRS.

*2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?*

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS requests. New user's Veterans Health Information Systems and Technology Architecture (VistA) ePAS request can include VistA menu options/security keys, Clinical Patient Record System (CPRS) access, etc. There are application-specific VistA menu option/security keys, and VistA role-specific configuration.

All VHA staff are responsible for assuring safeguards for the PII. Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly. VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current.

The system owner and managers are responsible for safeguarding PII/PHI

### **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*

Name (Last name, First Name, Middle Initial)  
Social Security Number  
Date of Birth  
Personal Mailing Address  
Personal Phone Number(s)  
Personal e-mail Address  
Health Insurance Beneficiary Numbers Account Numbers

Current Medications  
Previous Medical Records  
Race/Ethnicity  
Medical Record Number  
Other Unique Identifying Number (ICN Internal Control Number)  
Date of activity  
Attending Provider  
Education Order Results  
Admission Discharges and Transfers (ADTs)

### **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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule <https://www.archives.gov/records-mgmt/grs>? This question is related to privacy control DM-2, Data Retention and Disposal.*

Get Well Network (GWN) data is retained in accordance with the records disposition authority approved by the Archivist of the United States. The retention period for specific data will depend on which SORN that applies to that data. Here are the details for the SORNs this system uses:

SORN 79VA10, “Veterans Health Information Systems and Technology Architecture (Vista) Records-VA” <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf> states: Record Control Schedule (RCS) 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005–0004, item 020). RCS 10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006–0004, item 31).

SORN 24VA10A7, “Patient Medical Record-VA” <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf> states: “paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10-1, Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).”

RCS 10-1: <https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>.

### **3.3 The retention schedule 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. Please work with the system 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?*

All records are within the system of records indicated with disposition authority approved by the Archivist of the United States

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

As outlined in question 3.2 above record retention as it applies to data by SORN is as follows:

SORN 79VA10:

RCS 10-1, Item 2000.2, disposition authority DAA-GRS-2013-0005- 0004, item 020.

RCS 10-1, Item 2100.3, disposition authority DAA-GRS-2013-0006- 0004, item 31.

SORN 24VA10A7

RCS 10-1, Chapter 6, 6000.1d, disposition authority (N1-15-91-6, Item 1d) and 6000.2b (N1-15-02-3, Item 3).

RCS 10-1: <https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

### **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.*

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin.

Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)

### **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.*



Document Storage System (DSS) patches (VistA KIDS build) and Get Well Network (RPMs) are not released for National installation prior to testing. With an approved MOU (Memorandum of Understanding) from the IOC site(s), the vendor, Document Storage System (DSS) and Get Well. Test Patches are installed and tested in the VistA Pre-Production Test System. Get Well Network test RPMs are installed Pre-Production servers. IOC site(s) tester(s) complete the Test Site(s) User's Acceptance VistA Pre-Production System document prior to VistA Production System installation. Test patients are created in the VistA Pre-Production Systems to be used when testing new DSS Enterprise (DSI) Patches. VistA Pre-Production Systems test patients' data are scrambled.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

*Principle of Data Quality and Integrity: The PIA should describe 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:** PII or PHI may be held for longer than it is required to be maintained. This extension of retention periods increases the risk that information may be breached or otherwise put at risk of access by unauthorized persons.

**Mitigation:** The databases are encrypted, or the drive is encrypted. Access to these databases are restricted to only authorized users, administrative accounts. The standard user does not have access directly to the stored data.

To mitigate the risk posed by information retention, Get Well adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual's information is carefully disposed of. The individual's information is carefully disposed of following the procedures listed in 3.4.

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

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

### PII Mapping of Components

4.1a Get Well Network consists of three key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Get Well Network and the reasons for the collection of the PII are in the table below.

**Note:** Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

*Internal Components Table*

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
Veterans Health Information Systems and Technology (VistA)	Yes	Yes	Name (Last name, First Name, Middle Initial SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous	Patient Care	Encrypted

			Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity		
Get Well Government Server (GIS)	Yes	Yes	Name (Last name, First Name, Middle Initial), Gender, Date of Birth, Phone Number, Email, Admission Date, Discharge Date, Facility Code, Unit, Room, Bed, Order Number (Education & Medications), Education Code(s), Education Order Effective Date, Education Order Status, Medication (or NDC Code), Medication Administration, Attending Doctor, Medication Route, Appointment Type, Appointment Description,	Allow Get Well to deliver a customized and personalized patient experience to each Veteran, internet access, education services, as well as enable remote diagnostics, maintenance, monitoring, and repair updates by Get Well's technical support services.	No VA-sensitive information is transmitted from this dataflow direction. (All elements that may be considered sensitive are redacted and anonymized prior to transmission.)

			Appointment Duration, Appointment Date/Time, Event Reason, and Duration Unit.		
Oracle (GIS) Database	Yes	No	Obfuscates Patient ID, IEN, Encounter/Visit ID, First Name, Last Name, Gender, Date of Birth, Phone Number, Email, Admission Date, Discharge Date, Facility Code, Unit, Room, Bed, Order Number (Education & Medications), Education Code(s), Education Order Effective Date, Education Order Status, Medication (or NDC Code), Medication Administration, Attending Doctor, Medication Route, Appointment Type, Appointment Description, Appointment Duration, Appointment Date/Time,	GIS database consists of tables that support the transformation of an inbound HL7 message sent from VistA/CPRS from one that contains PHI to one that does not contain PHI for use by the Get Well's Patient Life System (PLS) server, Inpatient Module. In the reverse direction, the database supports the transformation of outbound HL7 messages from the Inpatient Application Server by re-inserting PHI information on messages to VistA/CPRS.	sensitive information is anonymized and stored with the non-sensitive information types

			Event Reason, and Duration Unit.		
--	--	--	----------------------------------	--	--

**4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.**

**NOTE: Question 3.9b (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*

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Veterans Health Information Systems and Technology (VistA)	The VistA system functions as the VA electronic health record (EHR) system. The comprehensive database within VistA provides a single source for Veteran patient data and the care and services available to the Veteran patient.	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control	HL-7 and RPC (Remote Procedure Call) Broker

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		Number), Date of activity, Event Type Code, Message Date Time, Patient ID, Encounter/Visit ID, Assigned Patient Location, Admission/Discharge Date Routing Code, Message to Send, & Date/Time of Message	
Get Well Government Server (GIS)	GIS receives inbound HL7 data feeds from VistA and obfuscates PHI using transformation rules before transmitting it to the GetWell Inpatient Module. GIS receives outbound data feeds from the Inpatient Application Server and re-inserts the corresponding PHI values by reversing the transformations before transmitting it to the facility VistA. In addition GIS receives REST Web Service calls from the meal ordering application in the GetWell Inpatient Module, re-identifies them and transmits them to the third-party meal ordering service. In the reverse direction, GIS receives REST Web Service calls containing dietary menu updates from the third-party meal ordering system	Name (Last name, First Name, Middle Initial), Gender, Date of Birth, Phone Number, Email, Admission Date, Discharge Date, Facility Code, Unit, Room, Bed, Order Number (Education & Medications), Education Code(s), Education Order Effective Date, Education Order Status, Medication (or NDC Code), Medication Administration, Attending Doctor, Medication Route, Appointment Type, Appointment Description, Appointment Duration, Appointment Date/Time, Event Reason	TCP – Internal VPN Bidirectional

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	and transmits these updates to the meal ordering application in the Inpatient Module.		
Oracle (GIS) Database	GIS database consists of tables that support the transformation of an inbound HL7 message sent from VistA from one that contains PHI to one that does not contain PHI for use by the GetWell Inpatient Module. In the reverse direction, the database supports the transformation of outbound HL7 messages from the Inpatient Application Server by re-inserting PHI information on messages to VistA.	Obfuscates Patient ID, IEN, Encounter/Visit ID, First Name, Last Name, Gender, Date of Birth, Phone Number, Email, Admission Date, Discharge Date, Facility Code, Unit, Room, Bed, Order Number (Education & Medications), Education Code(s), Education Order Effective Date, Education Order Status, Medication (or NDC Code), Medication Administration, Attending Doctor, Medication Route, Appointment Type, Appointment Description, Appointment Duration, Appointment Date/Time, Event Reason, and Duration Unit.	TCP - Internal VPN, Bidirectional. Support the transformation of an inbound HL7 message sent from VistA/CPRS from one that contains PHI to one that does not contain PHI. In the reverse direction, the database supports the transformation of outbound HL7 messages from the (External) Inpatient Application Server by re-inserting PHI information on messages to VistA
Computation Hospitality Suite TouchPoint Dining Gateway	Integrated with a meal ordering Web service application allows Veterans to order meal based on his/her dietary requirements	Medical Record Number Dietary menu updates	Bidirectional TCP

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).*

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

Follow the format below:

**Privacy Risk:** The privacy risk associated with maintaining PII/PHI is that sharing data within the Department of Veteran’s Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

**Mitigation:** The principle of need-to-know is strictly adhered to by the population Healthcare and non-Healthcare providers. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

## **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 List the external organizations (outside VA) that information shared/received, and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.**

**The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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

<p><b>List IT System or External Program Office information is shared/received with</b></p>	<p><b>List the purpose of information being shared / received / transmitted</b></p>	<p><b>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</b></p>	<p><b>List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</b></p>	<p><b>List the method of transmission and the measures in place to secure data</b></p>
<p>Get Well's Patient Life System (PLS) server, Inpatient Module</p>	<p>enables the VA to provide comprehensive Interactive Patient Care for Veteran patients. For VA care providers at a facility, the Inpatient Module allows these providers to prescribe customized health education to be delivered to a VA patient. For a Veteran patient, the Inpatient Module provides access to the GetWell Inpatient content, tools for service</p>	<p>Obfuscates Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Event Type Code, Message Date Time, Patient ID, Encounter/Visit ID, Assigned Patient Location, Admission Date Time.Set ID – ZNT, Routing Code, Message to Send, &amp; Date/Time of Message.</p>	<p>Get Well Network Inc MOU</p>	<p>SMTP, TCP and S2S VPN Tunnel</p>

	feedback, and the internet as well as resources that enable creation of a Personal Health Inventory and Plan.			
--	---	--	--	--

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** The privacy risk associated with sharing PII/PHI outside Department of Veteran’s Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

**Mitigation:** Get Well Network deploys a comprehensive information security program and performs annual security audits of its information systems. The results of the most recent audit performed by a third-party are available on request. Get Well employees receive annual mandatory information security training, as well as annual HIPAA training.

**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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of**

**the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**

*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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. All enrolled Veterans and Veterans who are treated at VA Medical Centers but not required to enroll are provided the VHA Notice of Privacy Practices (NoPP) every three years, or sooner if a change necessitates an updated notice. The NoPP is also prominently posted in every VAMC (posters) and on the VA public-facing website. Link to VHA NoPP: [https://www.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=9946](https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

Notice is also provided in the Federal Register with the publication of the following SORNs associated with this system:

SORN 79VA10 “Veterans Health Information Systems and Technology Architecture (VistA) Records–VA” <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>.

SORN 24VA10A7 “Patient Medical Record-VA” <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>.

*6.1b If notice was not provided, explain why.*

Notice was provided as indicated in question 6.1a above.

*6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.*

Please see the response to 6.1a above for details.

**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.*

Get Well Network extracts data that exists and was generated in the course of routine medical care. Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

### **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.*

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is provided. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

### **6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

*Principle of Transparency: This is referring to sufficient notice provided to the individual.*

*Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

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

**Mitigation:** This risk is mitigated by the common practice of providing the NoPP when Veterans apply for benefits. Additionally, new NoPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NoPP is also available at all VHA medical centers from the facility Privacy Officer.

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

## Section 7. Access, Redress, and Correction

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

### 7.1 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 [VA Public Access Link-Home \(efoia-host.com\)](http://www.foia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.*

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at <http://www.myhealth.va.gov/index.html>. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

The system is not exempt from Privacy Act provisions.

*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?*

The information in the system falls under Privacy Act systems of record and individuals have a right of access to request a copy of the information about themselves.

### 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.*

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

### **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.*

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NoPP) which states:

#### **Right to Request Amendment of Health Information.**

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call, or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and*

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.**

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

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record.

### **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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

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

**Principle of Individual Participation:** *The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

**Principle of Individual Participation:** *If access and/or correction is denied, then is the individual must be provided notice as to why the denial was made and how to challenge such a denial.*

**Principle of Individual Participation:** *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

**Mitigation:** The risk of incorrect information in an individual's records is mitigated by authenticating information, when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments. The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

### **8.1 The procedures in place to determine which users may access the system, must be 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?*

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application users have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training. Staff roles are determined by the VistA Person Class codes. Providers must have a valid Person Class in VistA File 200 (New Person) File. Local VHA site OI&T is responsible to complete the ePAS request. OI& Technical staff complete the ePAS approval for System Administrator (grant server access), Application Administrator (manage application), and/or VistA Management (manage VistA System related tasks)

Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training.

Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers.

Note: Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

*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?*

Other agencies do not have access to COTS Interface Division servers/applications.

*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.*

Get Well Network require application-specific VistA menu option(s) and/or VistA security key(s) to retrieve, create, and store data in VistA.

### **8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.**

*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.*

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Contractors and vendors do not have access to COTS Interface Division servers/applications

8.2a. Will VA contractors have access to the system and the PII?

Contractors and vendors do not have access to COTS Interface Division servers/applications

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors do not have access to COTS Interface Division servers/applications. Vendor provide RPM updates when available.

**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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

Organizational and non-organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

**8.4 The Authorization and Accreditation (A&A) completed for the system.**

*8.4a If completed, provide:*

1. *The Security Plan Status:* In Progress
2. *The System Security Plan Status Date:* In Progress
3. *The Authorization Status:* Not yet accessed.
4. *The Authorization Date:* In progress
5. *The Authorization Termination Date:* In Progress

6. *The Risk Review Completion Date: In Progress*

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 not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

ATO Authorization Date is In progress, but the application is in production since 2017.

## **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. (Refer to question 1.8 of the PTA)*

System does not use cloud technology.

### **9.2 Does the contract with the Hosting 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 3.3.1 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.**

System does not use cloud technology.

### **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.*

System does not use cloud technology.

**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.*

System does not use cloud technology.

**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).*

System does not use cloud technology.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Phillip Cauthers**

---

**Information Systems Security Officer, Roland Parten**

---

**Information Systems Owner, Gail Nemetz**

## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

### [VHA Notice of Privacy Practices IB 10-163p](#)

#### SORNs:

Veterans Health Information Systems and Technology Architecture (VistA) Records - VA  
79VA10 <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

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

## **HELPFUL LINKS:**

### **Records Control Schedule 10-1 (va.gov)**

#### **General Records Schedule**

<https://www.archives.gov/records-mgmt/grs.html>

#### **National Archives (Federal Records Management):**

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

#### **VA Publications:**

<https://www.va.gov/vapubs/>

#### **VA Privacy Service Privacy Hub:**

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

#### **Notice of Privacy Practice (NOPP):**

[VHA Directive 1605.04](#)

[VHA Notice of Privacy Practices IB 10-163p](#)