Privacy Impact Assessment for the VA IT System called:

LOGICARE Patient Instructions Traditional System
VHA

Date PIA submitted for review:

11/14/2022

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)	Richard Alomar-Loubriel and Crystal White	Crtystal.white5@va.gov, Richard.Alomar-Loubriel@va.gov	Richard: 787-696-4091, Crystal: 813-340-3089
Information System Owner	Rodney Sagmit	Rodney.Sagmit@va.gov	562-826-5789

Abstract

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

LOGICARE Patient Instructions is a healthcare information system which includes modules designed for both patient instruction and education. It is designed for use by clinicians to educate and instruct patients in emergency departments, inpatient units, and outpatient clinics. LOGICARE`s patient instructions are available to Veterans Affairs (VA) hospitals and clinics with Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS) integration. The LOGICARE System receives registrations/admissions from VistA to allow easy patient-selection by clinicians. Documents produced in LOGICARE for patients are contributed to the CPRS record as Notes. The instructions can include CPRS data from the patient`s record, particularly a current medication list, and a human readable list of future appointments.

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.

LOGICARE Patient Instructions. No Program Office is assigned, application is an existing

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

LOGICARE Patient instructions is a tool that is used to assigned diagnosis specific information to the patient, both print and video education

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

LOGICARE Patient Instructions is managed by the regional Commercial of-the-shelf (COTS) teams

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.

LOGICARE contain patient records for an estimated 1.5 million patient records across all instances of use

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

LOGICARE collected patient demographic information using an HL7 ADT feed received by CPRS. This patient demographic information is stored in our applications database, which all resides within the VA network. Any Patient Education assigned to the patient is also stored as part of their record in LOGICARE. Assigned education is documented back into CPRS using a custom HL7 ORU interface, which creates a signed NOTE in CPRS. LOGICARE maintains the patients email and smart phone number if patient request a link to assigned video education. This information is not required for patient to access assigned videos

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

None

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.*

LOGICARE Patient Instruction is operated at 36 VA hospital sites. This includes use in the ED, Inpatient, Medicine and Surgical Clinics. Each system has a separate ADT feed from VistA which provided site specific patient visit information (check in messages)

3. Legal Authority and SORN

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

.

SORN 24VA10A7 / 85 FR 62406 “Patient Medical Records-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.

SORN 79VA10 / 85 FR 84114 “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).

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?*

N/A

D. System Changes

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

An ATO has not been obtained in the past. No prior PIA document exists for application

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

No known changes expected

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)

Patient Secure Patient ID (GUID),
Patient Secure Visit ID (GUID),
Patient Future Appointment List,

Patient List of Education Assigned,
Patient Inpatient Room Number,
Patient Inpatient Bed Number,
LOGICARE Visit Area,
LOGICARE Visit Department,
LOGICARE Visit Facility,
CPRS Visit Location Code,
Patient Visit Account Number,
Patient Visit Arrival Date Time,
Patient Visit Registration DateTime,
Patient Visit Disposition DateTime ,
Patient Primary Care Doctor Full Name,
Patient Primary Care Doctor DUZ,
Application User Network login name,
Application User Medical Degree,
Application User Designated User Number (DUZ),
Application User Provider specialty,
Application User NPI (National Provider ID),
Secure Facility ID (GUID),

PII Mapping of Components (Servers/Database)

LOGICARE Patient Instructions consists of 20 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by LOGICARE Patient Instructions 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**
LC_SCRAPP1	**Yes**	**Yes**	**See paragraph below-** Patient Name, Patient Date of Birth, Patient Mailing Address,	**Required for Integration with CPRS, SSN is used to identify patient for matching encounter records**	**Advanced Encryption Standard (AES) 256, Server is stored in a secured environment with restricted access**

			Patient Phone Number, Patient Email, Patient Medical Record Number, Patient Social Security Number, Patient Integrated Control Number (ICN), Patient Gender, Patient Secure Patient ID (GUID), Patient Secure Visit ID (GUID), Patient Future Appointment List, Patient Medications, Assigned patient education for a given encounter of care, Patient Inpatient Room Number, Patient Inpatient Bed Number,		

			LOGICARE Visit Area, LOGICARE Visit Department, LOGICARE Visit Facility, CPRS Visit Location Code, Patient Visit Account Number, Patient Visit Arrival Date Time, Patient Visit Registration DateTime, Patient Visit Disposition DateTime , Patient Primary Care Doctor Full Name, Patient Primary Care Doctor DUZ, Application User Network login name, Application User Medical Degree, Application User Designated User Number (DUZ), Application User Provider specialty,		

			Application User NPI (National Provider ID), Secure Facility ID (GUID)		
LC_SCRAPP2	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_SCRAPP3	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_DVRAPP1	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_DVRAPP2	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_R2APPP01	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_R2PAPP02	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LC_R2PAPP03	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_EST1_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_EST2_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_ALN_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_WRX_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_COA_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_LEB_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_PHI_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_PTH_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_TOG_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_WBP_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_RIC_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**
LCARE_NJH_P	Yes	Yes	**Identical to above**	**Identical to above**	**Identical to above**

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?

Information is provided by VA approved HL7 ADT interface with CPRS

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.

Information is required to assign patient specific education to a patient and in return send education information back to CPRS using a HL7 interface in the form of a signed note. Any information received, but not processed is discarded from the database after 3 days. Patient Email and Mobile number are provided directly by patient and stored/maintained in LOGICARE Patient Instructions. Email and mobile numbers are only entered upon patient request as a method to access videos using a PIN protected URL link.

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

VistA/CPRS

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?

Information is received from an HL7 ADT interface as well as the VIA API tool, which includes the patient medication list and future appointment list from the Veteran medical record.

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.

No information is collected on paper copies

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.

Information stored in the application relies on updates provided by the HL7 interface with CPRS, all information is provided by CPRS, users do not enter official EHR patient information directly in LOGICARE. HL7 owned data is not editable in LOGICARE

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.

N/A

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

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

SORN 24VA10A7 / 85 FR 62406 “Patient Medical Records-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.

SORN 79VA10 / 85 FR 84114 “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).

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> VA Area Long Beach collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

<u>Mitigation:</u> System resides within the VA network and follows all standard OIT managed security safeguards.

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.

Data stored is used for the purpose of patient specific education reporting and tracking within the VA. This allows for application users to help identify educational goals and objectives

Name	
Patient Name	Used to identify a patient
Patient Date of Birth	Used to identify a patient
Patient Mailing Address	Used to identify a patient
Patient Phone Number	Used to Assign Video Education
Patient Email	Used to Assign Video Education
Patient Medical Record Number	Used to Identify Patient
Patient Social Security Number	Used to Identify Patient
Patient Integrated Control Number (ICN)	Used to identify patient with eVideon API Interface
Patient Gender	Used to identify a patient
Patient Secure Patient ID (GUID)	Used to identify patient when secure method required
Patient Secure Visit ID (GUID)	Used to identify patient encounter when secure method required
Patient Future Appointment List	Information included with printed discharge education, not discretely stored in application
Patient Medications	Information included with printed discharge education, not discretely stored in application
Assigned patient education for a given encounter of care	Education is assigned and data is tracked
Patient Inpatient Room Number	Used to identify a patient
Patient Inpatient Bed Number	Used to identify a patient
LOGICARE Visit Area	Allow patient to show in appropriate patient list and specific configurations
LOGICARE Visit Department	Allow patient to show in appropriate patient list and specific configurations
LOGICARE Visit Facility	Allow patient to show in appropriate patient list and specific configurations
CPRS Visit Location Code	Used to identify patient encounter and appropriate place them on a LOGICARE patient list
Patient Visit Account Number	Used to identify patient in application, not know to other systems
Patient Visit Arrival Date Time	Used to identify a patient encounter
Patient Visit Registration DateTime	Used to identify a patient encounter
Patient Visit Disposition DateTime	Used to identify a patient encounter
Patient Primary Care Doctor Full Name	Used to provide follow up instructions
Patient Primary Care Doctor DUZ	Used to provide follow up instructions
Application User Network login name	Login associated with PIV logged for authenticating users to application
Application User Medical Degree	Print with name on instructions

Application User Designated User Number (DUZ)	Required for CPRS integration to send education information back to CPRS (NOTE)
Application User Provider specialty	Used to help identify application user type
Application User NPI (National Provider ID)	Where applicable used on printed RX forms
Secure Facility ID (GUID)	Used with external API to identify a facilities (VA sites) content library asset

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.

None

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.

Facility, Department and patient level analysis data is available for reporting the level of education being assigned to a patient as well as the outcome of that education. This data is used to better understand when and if the patient is receiving education and can be correlated to patient satisfaction and other indicators

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?

VA manages the storing of data, as it exists on the VA OIT support hardware. This is done using VA standards including encryption of the SQL databases

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

VA manages the storing of data, as it exists on the VA OIT support hardware. This is done using VA standards including encryption of the SQL databases

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

VA manages the storing of data, as it exists on the VA OIT support hardware. This is done using VA standards including encryption of the SQL databases

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?

LOGICARE patient Instructions has its own security levels set along with audit controls, which audit user access to patient records.

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

Access audit/reporting are available in the application

2.4c Does access require manager approval?

Access to the application is determine by Active Directory security groups

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

Access audit/reporting are available in the application

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

Applications roles restrict certain access to information. VA manages the storing of data, as it exists on the VA OIT support hardware. This is done using VA standards including encryption of the SQL databases

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	
Patient Name	Stored – EHR owns data (not maintained in app)
Patient Date of Birth	Stored – EHR owns data (not maintained in app)
Patient Mailing Address	Stored – EHR owns data (not maintained in app)
Patient Phone Number	Stored – Maintained by App (not sent back to EHR)
Patient Email	Stored – Maintained by App (not sent back to EHR)
Patient Medical Record Number	Stored – EHR owns data (not maintained in app)
Patient Social Security Number	Stored – EHR owns data (not maintained in app)
Patient Integrated Control Number (ICN)	Stored – EHR owns data (not maintained in app)
Patient Gender	Stored – EHR owns data (not maintained in app)
Patient Secure Patient ID (GUID)	Stored – for in app use only
Patient Secure Visit ID (GUID)	Stored – for in app use only
Patient Future Appointment List	Stored – As snapshot in education document, not stored as discrete data
Patient Medications	Stored – As snapshot in education document, not stored as discrete data
Assigned patient education for a given encounter of care	Education is assigned and data is tracked
Patient Inpatient Room Number	Stored – EHR owns data (not maintained in app)
Patient Inpatient Bed Number	Stored – EHR owns data (not maintained in app)
LOGICARE Visit Area	Stored – for in app use only
LOGICARE Visit Department	Stored – for in app use only
LOGICARE Visit Facility	Stored – for in app use only
CPRS Visit Location Code	Stored – EHR owns data (not maintained in app)
Patient Visit Account Number	Stored – for in app use only
Patient Visit Arrival Date Time	Stored – EHR owns data (not maintained in app)
Patient Visit Registration DateTime	Stored – EHR owns data (not maintained in app)

Patient Visit Disposition DateTime	Stored – EHR owns data (not maintained in app)
Patient Primary Care Doctor Full Name	Stored – EHR owns data (not maintained in app)
Patient Primary Care Doctor DUZ	Stored – EHR owns data (not maintained in app)
Application User Network login name	Stored – for in app use only
Application User Medical Degree	Stored – for in app use only
Application User Designated User Number (DUZ)	Stored – EHR owns data (not maintained in app)
Application User Provider specialty	Stored – for in app use only
Application User NPI (National Provider ID)	Stored – for in app use only
Secure Facility ID (GUID)	Stored – for in app use only

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.*

LOGICARE Patient Instruction data is maintained for an unlimited time frame. Only log and other non-PHI related information is removed from the database as part of a maintenance process. LOGICARE does not produce any physical copies intended for the Patient Record.

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

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

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

Yes.

The information sent back to the Veteran medical record is retained for the life of that record as specified in the VHA Records Control Schedule (RCS 10–1) 6000.1d(N1–15–91–6, Item 1d) and 6000.2b(N1–15–02–3, Item 3).

Employee and trainee information is maintained under the records control specified for VISTA:

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, 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).

(also founder under help links section)

Record Control Schedules: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

LOGICARE Patient Instruction data is maintained for an unlimited time frame. Only log and other non-PHI related information is removed from the database as part of a maintenance process. LOGICARE does not produce any physical copies intended for the Patient Record. Information returned to the medical record is maintained in accordance with 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), Item 2100.3.

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.

LOGICARE does not produce any physical copies intended for the Patient Record.

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.

PII is not used for testing, research, or training purposes. We use the standard test patient practices of using ZZ as the last name to prevent real patient PII. Only ZZ test patients are used for any required testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: LOGICARE Patient Instructions collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: Users are granted access to the LOGICARE Patient Instructions application utilizing the users PIV card. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System.

OIT manages all security related activities as it relates to Operating System Security, or Database Security. All Hardware and OS software utilized by LOGICARE Patient Instructions is owned and managed by VA OIT in the VA network

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration - VistA	Allows for patient specific education to be assigned and tracked to the patient	*Patient Name,* *Patient Date of Birth,* *Patient Mailing Address,* *Patient Medical Record Number,* *Patient Social Security Number,* *Patient Integrated Control Number (ICN),*	*Electronically pulled from VistA thru Computerized Patient Record System (CPRS) us HL7 Interface*

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 Gender, Assigned patient education for a given encounter of care, Patient Inpatient Room Number, Patient Inpatient Bed Number, CPRS Visit Location Code, Patient Visit Arrival Date Time, Patient Visit Registration DateTime, Patient Visit Disposition DateTime , Patient Primary Care Doctor Full Name, Patient Primary Care Doctor DUZ	
Veterans Health Administration - VIA (Veterans Integration Adapter)	Allows instructions to also include the patient medication and future appointment list as part of the discharge instructions	*Current Medication List, Future Appointment List, Application User Designated User Number (DUZ)*	*VIA API Calls*
eVideon	Allows for the assigning of education to the eVideon in room TV	*Patient CPRS ICN, Secure patient identifier (GUID), Assigned patient education for a given encounter of care*	*JSON API call*

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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: LOGICARE Patient Instructions collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: There is no direct access to transmission of data. We utilize a least privilege/need to know policy for access.

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***
The Wellness Network Video Assignment Server	Tracks Video education assigned to patient	Non-PHI auto generated encrypted Patient ID (not the Medical Record ID)	BAA	https – API Get Only
The Wellness Network Video Mobile Assignment Server	Tracks Video education assigned to patient	Non-PHI auto generated encrypted Patient ID (not the Medical Record ID)	BAA	https – API Get Only
The Wellness Network Video Asset Management Server	Manages Site ID Asset Alllowances	Non-PHI auto generated encrypted Facility (VA site) ID	BAA	https – API Get Only
eVideon	Assign education to inroom VA tvs	Non-PHI auto generated Patient ID, List of Education Assigned to ID	None, eVideon has an MOU with Long Beach VA	https – API Get Only

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data outside of 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: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

.

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.

Veterans are provided with a copy of the VA Notice of Privacy Practices: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 24VA10A7 / 85 FR 62406 “Patient Medical Records-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.

SORN 79VA10 / 85 FR 84114 “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).

This Privacy Impact Assessment will also serve as a notice: https://www.oprm.va.gov/privacy/pia.aspx

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.

See 6.1a

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.

At the time of collection, individuals can decline a request to provide information. For instance, individuals have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN. The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their patient rights (i.e., to request a restriction).

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.

VHA permits individuals to agree to the collection of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. The VHA Notice of Privacy Practices provides information on the uses and disclosures of information that require their authorization. Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Risk that Veterans and other members of public will not know that the Logicare-Patient Information system exists or that if it collects or disseminates PII.

Mitigation: This PIA will be posted online for the public to view. All information collected comes from VistA/CPRS/EHR and VISTA. NOPP (Notice of Privacy Practice) are discussed at the individual VistA/CPRS/EHR sites and documented in their respective PIAs.

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.***

Data is entered or communicated to the VistA/CPRS/Unified EHR and the VistA/CPRS/Unified EHR is governed by VA policies and procedures for patient access to that data. VHA Release of Information (ROI) offices at facilities are present to assist Veterans with obtaining access to their health records and other records containing personal information. VHA established the MyHealthVet (MHV) program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features. In addition, Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended when appropriate.

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.

Procedures for an individual submitting an amendment to their health records are addressing VHA Directive 1907.01 and 1605.01. Both policies outline the rights of an individual to request an amendment to any information or records retrieved by the individual's name or other individually identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR. The request must be in writing over the signature of the individual and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer where the Veteran receives care to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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 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. The users would not have direct access to the medical devices/systems information to allow for corrections, and any information would be within the VistA/CPRS/Unified EHR. In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended when appropriate.

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.

The Veteran would utilize the procedures in the NOPP, which every patient receives when they enroll for care. The users would not have direct access to the medical devices/systems (eCareManager) information to allow for corrections, and any information would be within the VistA/CPRS/Unified EHR. In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended when appropriate. Inaccurate information is corrected by VA site personnel with access to the appropriate the VistA/CPRS/Unified EHR

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: Documentation of education assigned to patients does not process and record to CPRS as expected, resulting in CPRS not having a complete record.

Mitigation: Patients would follow the FOIA process, at which point a LOGICARE administrator would verify the training was assigned and completed. Any required updates would require an addendum action in CPRS.

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.

User are adding using established network security groups, a PIV card is required for access. Users can also be added directly to the application for access, however PIV authentication is still required. Users cannot log in with a separate username and password.

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?

Vendor support staff have access to the application. Those users are also VA contractors with established VA access

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.

Clinical Users are placed in a security group which allows them role based access to assign education. Clinical users are able to run pre-defined reports. No stored patient data from the EMR can be modified in the application.

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.

LOGICARE Patient Instructions contractors are VA credentialed employees and follow the same processes related to HIPPA training. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System.The vendor has an established BAA

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.

LOGICARE Contactors follow standard PIV card training requirements

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

No
8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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

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

2/21/2012

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)*

Application is currently installed on VA maintained VM servers located within various VA data centers

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A – Not cloud based

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A – Not cloud based

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A – Not cloud based

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

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

N/A – Not cloud based

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

ID	Privacy Controls
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.01.20 08:59:44 -08'00'

Privacy Officer, Phillip Cauthers

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2023.01.20 20:26:54 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

RODNEY A. SAGMIT 123726

Digitally signed by RODNEY A. SAGMIT 123726
Date: 2023.01.25 14:50:25 -08'00'

Information System Owner, Rodney Sagmit

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).

Veterans are provided with a copy of the VA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 24VA10A7 / 85 FR 62406 “Patient Medical Records-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.

SORN 79VA10 / 85 FR 84114 “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).

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