Privacy Impact Assessment for the VA IT System called:

Computrition Hospitality Suite

Veterans Health Administration (VHA)

Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

7/20/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Albert Comple	Albert.Comple@va.gov	318-229-9860
Information System Owner	Tony Sines	Tony.sines@va.gov	316-249-8510

Abstract

Computrition is a software package designed to facilitate food service in health institutions through various integrated modules for inventory management, menu management, meal planning, diet management while providing enhanced functionality to patients with a variety of room service options. Computrition integrates with most major electronic health record and manage systems utilizing industry standard interfaces, while also providing an interface to allow 3rd party Commercial Off The Shelf (COTS) products used by the VA as listed in table 4.1 to access and utilize specific Computrition functionality to incorporate additional functionality.

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.

Computrition Hospitality Suite: Enterprise Program Management Office (EPMO)

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

Computrition is used in over 130 Veteran Health Agency (VHA) facilities in Nutrition and Food Service (NFS) and managed under the auspice of Enterprise Program Management Office (EPMO). Computrition is a Citrix-based application that is incorporated as part of the GSS for former regions 1, 2 3 and 4. Computrition and its modules have been vetted through TRM (Technical Review Model) processes. The completion of this PIA will not result in any business or technology changes Computrition does not utilize Cloud technology. The number of individuals with information stored would vary by facility. Computrition will store Personally Identifiable Information (PII)/ Protected Health Information (PHI) for inpatient veterans whose information is received from the Department of Veteran Affairs (VA) Electronic Health Record (EHR) systems, throughout this document EHR represents VistA. Only patient information stored are those actively admitted as inpatient. Computrition has several modules utilized by VHA sites across the country:

• Food Operations Manager (FOM): Computrition offers a wide array of enterprise-level software features and services that help efficiently plan, organize, and manage production, inventory, and ordering operations. Computrition delivers superior management functionality and reporting options, gives access to valuable information that is virtually impossible to collect in a non-automated environment.

• Cost savings/Reduced waste: Store a history of post meal counts to assist in forecasting future production and order amounts; scale recipe and menu amounts according to production needs Improved nutrition quality for Veterans: Analyze nutrient information at the food item, recipe, and menu level; ability to populate nutrition labels for patient education and display in cafeterias. Staff workflow efficiencies: Implement order entry interfaces with major vendors; Update vendor item prices automatically that reflect costs at the food item, recipe, and menu level; Merge information from a master set of data out to site; save reports in a variety of Windows formats.

• Nutrition Care Management (NCM): streamlines workflow with the automation of manual processes. Administering an electronic patient cardex and better managing tray tickets and diet orders are just a few fundamental improvements. Having preventative food safety measures in place is vital in eliminating the risk of errors, harmful reactions or even fatal outcomes related to food allergies. NCM equips nutrition services to practice patient safety with features that can trigger alerts, customize tray tickets and modify menus to guarantee the food served coincides with the patients existing diet order. All patient information is securely transmitted across the one-way interface between VA EHR and Computrition. Improved safety/quality of Veteran nutrition care: Menu correction for food/drug interactions; Track diet order history; Ensure that patients are never served food that they dislike, are allergic to or that are inappropriate for their diet order; improved patient satisfaction scores. Staff workflow efficiencies: Redirect staff resources due to elimination of manual processes; ability to populate detailed reports to improve nutritional quality, safety and variety of menu items.

• Bedside Connect: Bedside Connect is an add-on module takes advantage of a tablet with touch screen abilities so that the bedside meal selection experience is easy and efficient for the user and quick and pleasant for the patient. Improved safety/quality of Veteran nutrition

care: Increases patient-staff interaction, helping to boost satisfaction scores; Take bedside patron meal orders using a tablet, Nutrition information is available to give patients feedback on their meal selections and can aide as a teaching tool for encouraging healthy meal choices. Staff workflow efficiencies: Significantly expedites the meal selection process; Flags selections for likes, dislikes, and allergies with the ability to enter them on the spot; find out who hasn't ordered their meal(s) yet, ensuring that your staff visit those patients and gather their selections. • Touch Point Dining: This add-on module will allow patients to order meals on their TV via the GetWellNetwork or other TV systems on the patients preferred schedule not dependent on any staff being in the room.

• Improved safety/quality of Veteran nutrition care: improves patient satisfaction scores; Nutrition information is available to give patients feedback on their meal selections and can aide as a teaching tool for encouraging healthy meal choices; Menus specific for patients with allergies and restricted food items removed, ensuring that menu offerings are appropriate for their therapeutic diets. Staff workflow efficiencies: Reduce the number of patients needing staff to visit to order meals.

• Cost savings/Reduced waste: Diminish food waste by delivering food that patients request; Increase labor savings by decreasing diet office staff required to operate a room service call center; Reduce the cost of and reliance on paper menus

• Room Service: Room service is an add-on module based on the hotel model, patients can similarly place an order from their room by selecting items from a restaurant-style menu, typically delivered within 45 minutes of ordering. Patient can order what they want (within diet restrictions), how they want it, when they want it. Improved safety/quality of Veteran nutrition care: flexibility in meal service, increasing patient satisfaction, improved food intakes and nutritional status due to Veterans being served the foods they prefer; Nutritional analysis includes patient meal intake calculations. Cost savings/Reduced waste: less food waste since the Veteran receive the foods they want/like versus items that are part of a standard menu that may not meet their preferences.

• Tray in Motion: Tray in Motion is an add-on module that is a real-time, integrated application enabling staff to efficiently manage tray delivery and retrieval of patient meals. A tool that utilizes barcode scanners with numerous benefits, Tray In Motion promotes patient safety by ensuring that the right meals are delivered in a timely manner to specific patients. It acts as a safeguard against delivery of an incorrect therapeutic diet and enables Nutrition Services teams to track and benchmark their individual and shift delivery times. Improved safety/quality of Veteran nutrition care: Acts as a safeguard against delivery of an incorrect therapeutic diet, increased patient satisfaction. Staff workflow efficiencies: Provides immediate tray delivery information to diet office staff and improves the meal delivery process flow and exposes areas that delay the tray transit time.

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

Veterans' Health Administration (VHA)

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.*

28,000 Individuals

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

Computrition Hospitality Suite (HS) is a minor application suite utilized at over 130 VA medical centers. HS is designed to streamline both food and nutrition operations in a multitude of hospitality sectors. While data is stored in Computrition, all medical information is extracted from the VA Electronic Health Record System (VistA or Cerner) and is not collected by Computrition.

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

Information is shared with GetWell Network (GWN) and Evideon to allow in- patients to order meals via in room equipment.

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.*

The system is maintained with a server cluster in the Austin Data Center to support the VA Medical Centers in the west. A second server cluster in the Philadelphia Data Center to support the VA Medical Centers in the east. Policies and procedures are managed by the Commercial of the Shelf (COTS) team.

3. Legal Authority and SORN

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

Under SORN 24VA10A7 Patient Medical Records – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.

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?*

No *to both questions*

D. System Changes

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

No

K. *Whether the completion of this PIA could potentially result in technology changes*
No

Section 1. Characterization of the Information

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

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

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

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

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

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

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

- Admission date
- Discharge date

- Diet orders from Electronic Health Record
- Allergies
- Special order
- Religion
- Reason for visit
- Diagnosis
- Language spoken

PII Mapping of Components (Servers/Database)

Computrition Hospitality Suite has 4 databases that stores patient data. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Computrition Hospitality Suite and the reasons for the collection of the PII are in the table below**.**

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
HSWESTV	**No**	**Yes**	Social Security Number, Name, Date of Birth, Medical Record Number, Admission/Discharge Date, Diet Order, Allergies, Diagnosis	Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.	Database servers are encrypted and fully compliant with VA Database baseline standards.
HSWESTC	**No**	**Yes**	Social Security Number, Name, Date of Birth, Medical Record Number, Admission/Discharge Date, Diet Order, Allergies, Diagnosis	Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods	Database servers are encrypted and fully compliant with VA Database baseline standards.

				they are allergic to.	
HSEASTV	**No**	**Yes**	Social Security Number, Name, Date of Birth, Medical Record Number, Admission/Discharge Date, Diet Order, Allergies, Diagnosis	Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.	Database servers are encrypted and fully compliant with VA Database baseline standards.
HSEASTC	**No**	**Yes**	Social Security Number, Name, Date of Birth, Medical Record Number, Admission/Discharge Date, Diet Order, Allergies, Diagnosis	Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.	Database servers are encrypted and fully compliant with VA Database baseline standards.

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?

VA EHR is the source of information for Computrition. The information in Computrition is pushed from the VA EHR to Computrition via a unidirectional Health Level 7 (HL7) interface. Updates to information must be made in the VA EHR and pushed to Computrition via the same unidirectional HL7 interface.

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 VA EHR is the permanent System of Records for all information. Computrition utilizes VA EHR as their source.

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

Computrition does not create any original information.

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?

All information is provided by the Electronic Health Record via HL7 interface to Computrition and verified during patient contact.

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.

N/A

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.

Sites are encouraged to check accuracy of all information that comes across the interface. Sites have been encouraged to compare diet orders in Computrition to VA EHRM for discrepancies. Computrition information is used in conjunction with existing data from VA EHRM. The information collected is a combination of Personal Identifiable Information (PII) and Protected Health Information (PHI).

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

SSN serves as the Medical Record Number and Unique Identifier for the Veteran and is collected by the VA EHR which then pushes the information to Computrition. The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs. Also to include Title 38, United States Code, Sections 501(b) and 304; and Title 38, United States Code, section 7301(a).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Privacy Risk: The Computrition software suite collects both 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: Veterans Health Administration (VHA) deploys extensive security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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.

- Name: Used to identify the patient and verify diet orders, allergies and in other forms of communication
- Social Security Number: Used as a patient identifier
- Date of Birth: Used to identify age and confirm patient identity
- Medical Records: Used to keep record of medical information
- Medical Record Number: Used as a patient identifier in Computrition
- Gender: Standardly interfaces with Computrition
- Integrated Control Number (ICN): Interfaces from Cerner and allows us to look them up in Cerner when trouble shooting issues to ensure we have the correct patient.
- Diet orders from Electronic Health Record: Critical to ensure the kitchen is providing the appropriate food to the patient.
- Special order: Sends information such as if the patient is in isolation (kitchen needs to know if the items need to be on paper for infection control purposes or if staff should not enter a room to deliver the meal), Self-Harm Order (kitchen needs to know so they send the appropriate tray that does not have items that could be used to harm the patient such as metal forks, china dishes that could be broken), Early Trays/Late Trays (if the patient needs their tray held because they are having a test over a meal time), and meal selection (notifies the kitchen if a patient will be making meal selections with room service style vs receiving the house tray).
- Religion: Some religions may impact the patient's diet such as no pork or no meat during Lent.
- Reason for visit: Standardly interfaces with Computrition
- Diagnosis: Standardly interfaces with Computrition

- Language spoken: kitchen would need to know if there might be a language barrier when getting meal selections from the patient.
- Admission Date: To notify the kitchen of a new admission and need for a tray
- Diet Order from CPRS: The kitchen needs to know what the patients diet order is to ensure safe meal delivery to patient.
- Allergies: Ensure patients are not fed food they are allergic to.

.

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.

Computrition does not analyze patient data.

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.

N/A

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?

Database servers are encrypted and fully compliant with VA Database baseline standards.

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

No

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

Each NFS service has system administrators who maintain access to Computrition and ensures safeguards of PII/PHI. It is the responsibility of NFS to ensure that employees who have Computrition access within the service stay current on required HIPPA and Privacy training, otherwise access to the computers are removed.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to Computrition is controlled at the local site level using approval processes defined by the local site Nutrition and Food Services (NFS) department. Inside of Computrition, each site works with the vendor to build a customized series of "security levels" that allows them to build multiple levels of authorization appropriate to the data access requirements of individual jobs. Each Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

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

Each Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

2.4c Does access require manager approval?

Each Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

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

No

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

Each Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The information listed in Section 1.1 is retained in the Computrition database and is deleted based upon the Records Control Schedule (RCS).

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.

The data retention period has been approved by NARA and is processed according to the following:
- Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf
- National Archives and Records Administration: www.nara.gov

According to Records Control Schedule 10-1 , (See page 251 and 252 of RCS 10-1) the information is considered Temporary and the disposition depends on information in Computrition.

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

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

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

Computrition is not a System of Record. The VA EHR is the system of Records for all information retained in Computrition.

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

The data retention period has been approved by NARA and is processed according to the following:
Records Control Schedule
• National Archives and Records Administration: www.nara.gov.

According to Records Control Schedule 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). Records Control Schedule 10-1 (va.gov)

the information is considered temporary and the disposition depends on information in Computrition.

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.

An automated process runs each day to remove information that meet or exceed retention timeframe criteria. Data contained in Computrition can be manually removed if necessary, based upon the disposition in RCS 10-1.

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.*

Computrition does not use PII for research, 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: The risk to maintaining data within the Computrition system is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness & Rules of Behavior training annually. Computrition adheres to all information security requirements instituted by the VA Office of Information and Technology (OI&T). RCS 10-1 is being followed, as approved by NARA.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Vista	To enable authorized personnel to view Veteran's Patient information in a timely manner.	PII-PHI as identified in section 1.1 • Name • Social Security Number • Date of Birth • Medical Record Number • Other Unique Identifying Number • Admission date • Diet orders from Electronic Health Record • Allergies	Unidirectional HL7 interface from Vista to Computrition
GetwellNetwork (GWN)	To allow patients to order room service from their television.	• Medical Record Number	Hospitality Suite xChange Gateway

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***
eVideon	To allow patients to order room service from their television.	• Medical Record Number	Hospitality Suite xChange Gateway

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:

<u>Privacy Risk:</u> There is a risk that information may be shared with unauthorized VA programs or systems or that data could be shared inappropriately.

<u>Mitigation:</u> 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 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: no risk as system does not share information outside of the Department.

Mitigation: N/A

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.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR and SORN.

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

Notice is also provided in the Federal Register with the publication of the SORN: 2020-21426.pdf (govinfo.gov)

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

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

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

Notice was provided as stated in 6.1a above

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

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

Information 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.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

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

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Example Privacy Risk:</u> 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.

<u>Mitigation:</u> 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 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.***

Information in Computrition is populated by the EHR 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 https://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).

Computrition receives all data from VA EHR and this would be covered in the applicable SORN for the designated EHR.

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.

Computrition receives all data from VA EHR and this would be covered in the applicable SORN for the designated EHR.

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.

Computrition receives all data from VA EHR and this would be covered in the applicable SORN for the designated EHR.

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.

Computrition receives all data from VA EHR and this would be covered in the SORN for the designated EHR.
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

7.4 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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Computrition receives all data from VA EHR and this would be covered in the applicable SORN for the designated EHR. Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3In addition to the formal procedures discussed in question 7.2 to request changes to one's health record, a veteran or other VAMC patient who is enrolled in myHealthevet can use the system to make direct edits to their health records

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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: There is a risk that individuals are unaware of how to access or correct their information in the system.

Mitigation: Computrition receives all data from VA EHR and this would be covered in the applicable SORN for the designated EHR. Information in the system is only collected from other systems. Access, redress, and correction procedures are provided by the source systems and outlined in the SORN

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.

Each Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

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?

N/A

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.

- Manager – Global Administrators limited to OIT COTS team members
- *User Admin – Local site administrators that manage users and security levels*

- *Users – Standard users may be limited to individual areas of the application based on job assignment and duty requirement*

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.

Computrition and the VA ensure that all personnel including contractors who have access to VA computers must complete the onboarding and annual Privacy and Information Security Awareness mandatory training. Contracts are reviewed by the appropriate contract authority i.e., Contracting Officer Representative (COR), Contracting Officer (CO), Contract Review Committee. Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VA HIPAA Privacy Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

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

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

All VA employees who have access to VA computers must complete the onboarding and annual mandatory Privacy and Information Security Awareness Training. In addition, all employees who interact with patient sensitive medical information must complete the mandated VHA HIPAA Privacy Training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject-specific training on an as needed basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date: Reviewed 6/15/2023*
3. *The Authorization Status:* 3 Year ATO
4. *The Authorization Date:* 6/10/2022
5. *The Authorization Termination Date:* 6/9/2025
6. *The Risk Review Completion Date:* 6/3/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

Section 9 – Technology Usage

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

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

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

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

No

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

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

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

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

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.07.31 11:44:05 -04'00'

Privacy Officer, Nancy Katz-Johnson

ALBERT COMPLE

Digitally signed by ALBERT COMPLE
Date: 2023.07.29 12:45:53 -06'00'

Information System Security Officer, Albert Comple

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2023.07.31 10:56:08 -05'00'

Information System Owner, Tony Sines

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).

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR and SORN.

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

Notice is also provided in the Federal Register with the publication of the SORN: 2020-21426.pdf (govinfo.gov) SORN 24VA 10A7 Patient Medical Records - VAAUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.

HELPFUL LINKS:

Record Control Schedules:

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

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

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

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices