Privacy Impact Assessment for the VA IT System called:

Somnoware- Enterprise

Veterans Health Administration (VHA)

Office of Connected Care (OCC)

eMASS ID #1288

Date PIA submitted for review:

10-3-2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.Lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Matthew Hester	Matthew.Hester@va.gov	217-554-3134
Information System Owner	Ray Dennis	Ray.Dennis@va.gov	561-788-0182

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Somnoware- Enterprise is a respiratory workflow management platform designed to accelerate the diagnosis of Obstructive Sleep Apnea (OSA) and Chronic Obstructive Pulmonary Disease (COPD) and improve patient treatment outcomes. By integrating with over 150 applications, diagnostic devices, and treatment appliances Somnoware-e unifies disparate data within a single web-based application. Clinicians can diagnose patients 40% faster, identify their at-risk populations, and track patient Positive Airway Pressure (PAP) adherence.

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. *What is the IT system name and the name of the program office that owns the IT system?*
The Somnoware-e system is owned and operated by the providing SaaS vendor Somnoware-e, a cloud based Respiratory care SaaS platform and will be controlled by the Veterans Health Administration (VHA) Office of Connected Care (OCC).

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
Somnoware-e will standardize the quality of care across VHA's national sleep and pulmonary medicine program. This web-based platform will allow us to diagnose patients faster, monitor treatment progress, and automatically exchange data with our Veterans Health Information Systems and Technology Architecture (VistA), Computerized Patient Record System (CPRS), and Cerner electronic health records (EHR). We estimate that 120,000 Veterans whose information will be stored in Somnoware-e, will benefit from this System. The beneficiaries are 1. Providers: Sleep studies and pulmonary function tests will be interpreted by Version Date: May 1, 2021 Page 2 of 32 providers through Somnoware-e. 2. Patient: Once the patient is diagnosed with sleep apnea or Chronic Obstructive Pulmonary Disease, patient adherence will be managed and improved by using Somnoware-e. 3. VA System: VHA spends 300 million dollars a year on Continuous Positive Airway Pressure (CPAP) devices used as therapy devices for Veterans. Somnoware-e will keep checks and balances for this expenditure by the VA. All VA Medical Centers (VAMC) and Community Based Outpatient Clinics (CBOC) where there is Pulmonary or sleep physician, a respiratory therapist or Sleep technologist. Patient demographics ordered for a respiratory disorder namely sleep disorder, respiratory diseases, patient identifiers, Study data, technician notes, physician interpretation reports, questionnaires. Somnoware-e will be sending study reports, Questionnaire, therapy device adherence reports to (a) VistA CPRS and VistA Imaging via API over a site to site virtual

private network (VPN), (b) to Cerner via Health Level Seven (HL7) over site to site VPN; and Cerner, Remote Order Entry System (ROES) to a secure file transfer protocol (SFTP) site.

C. *Who is the owner or control of the IT system or project?*
The system is owned and operated by the providing SaaS vendor Somnoware-e, a cloud based Respiratory care SaaS platform and will be controlled by the Veterans Health Administration (VHA) Office of Connected Care (OCC).

2. Information Collection and Sharing

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*
It is anticipated there will be 900 users and 275,000 total Veterans impacted.

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*
Somnoware-e will standardize the quality of care across VHA's national sleep and pulmonary medicine program. This web-based platform will allow us to diagnose patients faster, monitor treatment progress, and automatically exchange data with our Veterans Health Information Systems and Technology Architecture (VistA), Computerized Patient Record System (CPRS), and Cerner electronic health records (EHR). We estimate that 120,000 Veterans whose information will be stored in Somnoware-e, will benefit from this System. The beneficiaries are 1. Providers: Sleep studies and pulmonary function tests will be interpreted by Version Date: May 1, 2021 Page 2 of 32 providers through Somnoware-e. 2. Patient: Once the patient is diagnosed with sleep apnea or Chronic Obstructive Pulmonary Disease, patient adherence will be managed and improved by using Somnoware-e. 3. VA System: VHA spends 300 million dollars a year on Continuous Positive Airway Pressure (CPAP) devices used as therapy devices for Veterans. Somnoware-e will keep checks and balances for this expenditure by the VA. All VA Medical Centers (VAMC) and Community Based Outpatient Clinics (CBOC) where there is Pulmonary or sleep physician, a respiratory therapist or Sleep technologist. Patient demographics ordered for a respiratory disorder namely sleep disorder, respiratory diseases, patient identifiers, Study data, technician notes, physician interpretation reports, questionnaires. Somnoware-e will be sending study reports, Questionnaire, therapy device adherence reports to (a) VistA CPRS and VistA Imaging via API over a site to site virtual private network (VPN), (b) to Cerner via Health Level Seven (HL7) over site to site VPN; and Cerner, Remote Order Entry System (ROES) to a secure file transfer protocol (SFTP) site.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*
Somnoware-e will be sending study reports, Questionnaire, therapy device adherence reports to VA Information systems medical record systems
(a) VistA, CPRS, and VistA Imaging via API over a site to site virtual private network (VPN),
(b) to Cerner via Health Level Seven (HL7) over site to site VPN; and Cerner,
(c) Remote Order Entry System (ROES) to a secure file transfer protocol (SFTP) site

G. Is 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?

Somnoware-e will be used across multiple healthcare facilities within the VA for sleep and respiratory healthcare diagnostics and therapy. Somnoware-e user manuals and trainings help and support VA clinicians to use the system effectively. Somnoware-e being a cloud application data across the sites are maintained securely and consistently.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The authority for this interconnection is based on: Federal Information Security Modernization Act of 2014 (FISMA 2014)VA Directive 6500, VA Directive 6500: VA Cybersecurity Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45C.F.R. Part 16038 United States Code (U.S.C.) §§ 5721-5728, Veteran’s Benefits, Information Security Office of Management and Budget (OMB) Circular A-130, Managing Information as Strategic Resource Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009),codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. Executive Order 9397 gives authority to collect and use the SSN as an identifier. Privacy Act System of Records Routine Uses in SORN - Patient Medical Record – VA 24VA10A7, SORN - Veterans Health Information Systems and Technology Architecture (VistA) Records – VA 79VA10, and SORN - National Patient Databases – VA 121VA10
https://www.oprm.va.gov/privacy/systems_of_records.aspx.
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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?

The SORN – National Patient Databases – VA for this system is 121VA10 and does not require updates.

4. System Changes

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

No changes to existing business process with this version on PIA.

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

Integration with Somnoware involves new system interconnections between VA systems and Somnoware FedRAMP authorized cloud. No changes foreseen due to this version of PIA. Somnoware-e is a cloud based Respiratory care SaaS platform sponsored by the Veterans Health Administration (VHA) Office of Connected Care (OCC). Somnoware-e will standardize the quality of care across VHA’s national sleep and pulmonary medicine program. This web-based platform will allow us to diagnose patients faster, monitor treatment progress, and automatically exchange data with our Veterans Health

Information Systems and Technology Architecture (VistA), Computerized Patient Record System (CPRS), and Cerner electronic health records (EHR). We estimate that 120,000 Veterans whose information will be stored in Somnoware-e, will benefit from this System. The beneficiaries are:
1. Providers: Sleep studies and pulmonary function tests will be interpreted by providers through Somnoware-e.
2. Patient: Once the patient is diagnosed with sleep apnea or Chronic Obstructive Pulmonary Disease, patient adherence will be managed and improved by using Somnoware-e.
3. VA System: VHA spends 300 million dollars a year on Continuous Positive Airway Pressure (CPAP) devices used as therapy devices for Veterans. Somnoware-e will keep checks andbalances for this expenditure by the VA. All VA Medical Centers (VAMC) and Community Based Outpatient Clinics (CBOC) where there is Pulmonary or sleep physician, a respiratory therapist or Sleep technologist. Patient demographics ordered for a respiratory disorder namely sleep disorder, respiratory diseases, patient identifiers, Study data, technician notes, physician interpretation reports, questionnaires. Somnoware-e will be sending study reports, Questionnaire, therapy device adherence reports to (a) VistA CPRS and VistA Imaging via API over a site to site virtual private network (VPN), (b) to Cerner via Health Level Seven (HL7) over site to site VPN; and Cerner, Remote Order Entry System (ROES) to a secure file transfer protocol (SFTP) site.
Somnoware-e has a VA Authority to Operate (ATO) and FedRAMP ATOs, including Department of Defense (DoD) requirements to connect to Cerner Federal Enclave which houses DoD data. The service agreement dictates ownership rights of data. The principle is described in contracts with the customer, this is described in Section 8.1 of the service agreement "Liability for Subject Data." To date Somnoware-e has not encountered any data breaches. The risk is categorized as Moderate. No restricted personal health information (PHI) are transferred to Somnoware-e. The data is limited to respiratory diseases namely Sleep Apnea and Chronic Obstructive Pulmonary Disease (COPD).

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. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ 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[1]
☐ 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)
Full list of items in section 2.1 below

Other PII/PHI data elements:

- Primary Physician NPI (National Provider Identifier)
- Sleep and pulmonary function Study Data – Interpretation and diagnosis
- Diagnosis Date – Diagnosis information
- questionnaire related to sleep and pulmonary function studies - Input to Diagnosis and Therapy
- Hospital Data - Input to Diagnosis and Therapy
- Date of Admit - Input to Diagnosis and Therapy
- Date of Discharge - Input to Diagnosis and Therapy
- Primary and Secondary Diagnosis Codes (ICD-10) - Input to Diagnosis and Therapy

PII Mapping of Components (Servers/Database)

Somnoware-e consists of two 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 Somnoware-e and the reasons for the collection of the PII are in the table below.

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

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
Somnoware-e Database	YES	YES	a. Name b. Social Security Number – Last 4 only c. Date of Birth d. Personal Mailing Address e. Personal Phone Number(s) f. Personal Fax Number g. Personal Email Address h. Internet Protocol (IP) Address Numbers – In audit logs i. Sleep and pulmonary function Study Data – Interpretation and diagnosis j. Questionnaire related to sleep and pulmonary function studies - Input to Diagnosis and Therapy	Patient Identification	Encryption, role based access and audit

			k. Hospital Data - Input to Diagnosis and Therapy l. Date of Admit - Input to Diagnosis and Therapy m. Date of Discharge - Input to Diagnosis and Therapy n. Primary and Secondary Diagnosis Codes (ICD-10) - Input to Diagnosis and Therapy		
Somnoware-e File Storage	YES	YES	a. Name b. Date of Birth c. Sleep and pulmonary function Study Data – Interpretation and diagnosis	Sleep study and pulmonary function test interpretation and diagnosis	Encryption, role based access and audit

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Data is collected from VA applications namely Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS), Cerner, VA Remote Online Order Entry System (ROES).

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.

Somnoware-e collects data from Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS), Cerner, VA Remote Online Order Entry System (ROES) to avoid duplication and maintain consistency.

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

The sources of the data points identified above are from VA applications namely Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS), Cerner, VA Remote Online Order Entry System (ROES). Somnoware-e will consume individual Health Level Seven (HL7) messages for patients or Application Programming Interface (API) calls for individual patients. Sleep Study and Pulmonary Function test data is collected from different diagnostic and therapy devices. Physicians use this data to generate diagnostic study interpretation reports. Somnoware-e is registered with the Food and Drug Administration (FDA) as medical device data (MDD) system. As part of the diagnostic study, the providers need Questionnaires completed by the patients. Somnoware-e facilitates this process eliminating paper.

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?

Somnoware-e will consume individual Health Level Seven (HL7) messages for patients or Application Programming Interface (API) calls for individual patients. Sleep Study and Pulmonary Function test data is collected from different diagnostic and therapy devices. Physicians use this data to generate diagnostic study interpretation reports.

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

Somnoware-e will consume individual Health Level Seven (HL7) messages for patients from Cerner and Application Programming Interface (API) calls for individual patients to Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS). Diagnostic Study data is collected from diagnostic devices via APIs developed by device manufacturers. The patient receives a link and uses this link from a computer or smart device to open a questionnaire. The patient questionnaire comprises of pre and post study questionnaires and patient survey. It collects information related to sleep and pulmonary function studies and information is used to help to diagnosis and therapy pathways.

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.

Unique Patient identifiers are transmitted via Health Level Seven (HL7) and Application Programming Interface (API). This Patient identifier is used across Somnoware-e in every step. A sleep study report generated in Somnoware-e is verified every time by the VA physician by reviewing the raw study data from the diagnostic study. A study report sent from Somnoware-e to VA Cerner or Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS)will contain the Patient unique identifier.

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

The system does not use commercial aggregators. Unique Patient identifiers are transmitted via Health Level Seven (HL7) and Application Programming Interface (API). This Patient identifier is used across Somnoware-e in every step. A sleep study report generated in Somnoware-e is verified every time by the VA physician by reviewing the raw study data from the diagnostic study. A study report sent from Somnoware-e to VA Cerner or Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS)will contain the Patient unique identifier.

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 authority for this interconnection is based on:

- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- VA Directive 6500, VA Directive 6500: VA Cybersecurity Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA
- Information Security Program
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45
- C.F.R. Part 160
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Managing Information as Strategic Resource
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. Executive Order 9397 gives authority to collect and use the SSN as an identifier.

- Privacy Act System of Records Routine Uses in Patient Medical Record – VA 24VA10A7,
    - Veterans Health Information Systems and Technology Architecture (VistA) Records – VA 79VA10
    - National Patient Databases – VA 121VA10
- SORN - https://www.oprm.va.gov/privacy/systems_of_records.aspx. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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> Loss of control of Personal Health Information (PHI) or Personally Identifiable Information (PII).

<u>Mitigation:</u> Personal Health Information (PHI) or Personally Identifiable Information (PII) is transmitted over secure channels that use strong encryption. Data stores are also encrypted using strong encryption such that individual users involved in maintenance of facility will not be able to access confidential data directly**.** The security of the information being passed on this connection must be protected through the use of FIPS 140-2 (or successor) validated encryption implemented according to the specifications in the validated modules certificate. The connections at each end are located within controlled access facilities using physical access devices and/or guards. Individual users will not have access to the data except through the system security software inherent to the operating system. Access is controlled by authentication methods to validate the approved users. The FIPS 140-2 certificate number of Somnoware-e gateway cryptographic module for establishing the Virtual Private Network (VPN) tunnel is FIPS# 3479.

Section 2. Uses of the Information

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

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

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

The information stored in Somnoware-e such as Personal Health Information (PHI) and Personally Identifiable Information (PII)will be instrumental in helping physicians diagnose obstructive sleep apnea and chronic obstructive pulmonary disease at an accelerated rate. By aggregating these clinical and demographic data points in Somnoware-e's database, sleep physicians can generate interpretation reports more accurately and track treatment progress of all patients from a single web-based solution. The time to diagnose a Veteran with respiratory illness and have them begin treatment will be shortened significantly as well. Below is a list of Personal Health Information (PHI) and Personally Identifiable Information (PII):

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not used
Social Security Number (Last 4 digits only)	Identifying patient	Not used
Date of Birth	Identifying patient and calculating age	Not used
Personal Mailing Address	Device shipping	Not used
Personal Phone Number(s)	Contact and notification on sleep and respiratory appointments	Not used
Personal Fax Number	Contact and notification on sleep and respiratory appointments	Not used
Personal Email Address	Contact and notification on sleep and respiratory appointments	Not used
Internet Protocol (IP) Address Numbers	Auditing and Geo-blocking outside of United States of America	Not used
Current Medications	Input to diagnosis and therapy	Not used
Medical Record Number	Uniquely identify patient	Not used
Diagnostic study appointment dates (respiratory only)	Scheduling appointments in Somnoware-e	Not used

Sleep and pulmonary function Study Data	Interpretation and diagnosis	Not used
Diagnosis Date	Diagnosis information questionnaire related to sleep and pulmonary function studies – Input to Diagnosis and Therapy	Not used
Hospital Data	Input to Diagnosis and Therapy	Not used
Date of Admit	Input to Diagnosis and Therapy	Not used
Date of Discharge	Input to Diagnosis and Therapy	Not used
Primary and Secondary Diagnosis Codes (ICD-10)	Input to Diagnosis and Therapy	Not used

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?

Somnoware-e uses conditional logic to automatically apply physician phrasing to diagnostic study interpretation reports.

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.

The algorithms in Somnoware-e process clinical data acquired from the sleep/respiratory study against diagnostic conditions (parameters) configured by the clinician to eliminate manual entry when generating a report. The physician then reviews the report before finalizing the same. Finalized reports are sent to VA CPRS and ViSTA to be updated against the existing patient record.

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?

Both Data Storage and Data transmission use FIPS 140-2 certified encryption to secure the information.

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

The systems store only last 4 digits of Social Security Number (SSN) to enable SSN based searching.

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

Both Data Storage and Data transmission use FIPS 140-2 certified encryption to secure the information. The systems store only last 4 digits of Social Security Number (SSN) to enable SSN based searching.

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?

Somnoware-e uses Role based access. All users and processes are required to use unique identifiers to access and authenticate to the system. Access to system is provisioned by VA administrators bearing the Somnoware-e roles Centralized Administrators and Lab Managers.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes, the audit logs capture PII access.

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

Somnoware-e users and processes are required to use unique identifiers to access and authenticate to the system. The information system uses several factors to establish uniqueness and to achieve secure authentication. Authentication factors vary depending on the system component.

All Somnoware-e employees are assigned individual unique identifiers to access and authenticate to the environment. Each user is assigned a unique user ID, using the process detailed within the FedRAMP moderate System Security plan and Somnoware-e access control policy and procedures.
The Somnoware-e infrastructure is accessible to only a few individuals within the Somnoware-e organization. Somnoware-e uses Okta software to enforce multifactor authentication to the Amazon Web Service (AWS) environment. Additionally, network access to privileged accounts is allowed through virtual private network with Secure Socket Layer (SSL). All components are configured to enforce Somnoware-e's password policies. Somnoware-e Active Directory accounts are formatted using a standard convention.

VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI) governs the reporting of incidents involving VA systems and information. If Somnoware-e has an employee, contractor, or agent who becomes aware of the theft, loss or compromise of any device used to transport, access, or store VA sensitive information or data (See Appendix D); such employee, agent, or contractor must immediately report the incident to the VA Points of Contact (POC) listed within Appendix A, or in the Business Associate Agreement (BAA) or contract when applicable, so that the incident can be reported to the VA Cybersecurity Operations Center (VA-CSOC) for action. Should any security incident or event (or suspected incident or event) involve VA owned sensitive information (e.g. the theft, loss, compromise, or destruction of any device used to transport, access, or store VA sensitive information/data) covered by this agreement, or the incident places VA sensitive information/data at risk of loss, unauthorized access, misuse or compromise, then Iron Bow Technologies partner, Somnoware-e, will notify the VA point of contact (POC) listed within Appendix A, or in the BAA or contract when applicable, by phone or in writing (mail or email) immediately upon detection. The VA POC will immediately notify VHA Office of Connected Care's Information Systems Security Officer (ISSO) or Privacy Officer (PO) who will contact VA-CSOC within one hour of notification.

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 - For identifying patient
- Social Security Number (SSN Last 4 only) - For identifying patient
- Date of Birth - For identifying patient and calculating age
- Personal Mailing Address - Device shipping
- Personal Phone Number(s) - Contact and notification on sleep and respiratory appointments
- Personal Fax Number - Contact and notification on sleep and respiratory appointments
- Personal Email Address - Contact and notification on sleep and respiratory appointments
- Internet Protocol (IP) Address Numbers - Auditing and Geo-blocking put side of United States of America
- Current Medications - Input to Diagnosis and Therapy
- Medical Record Number - Uniquely identify patient
- Diagnostic study appointment dates (respiratory only) - Scheduling appointments in Somnoware-e
- Sleep Study and Pulmonary function test Data – Interpretation and diagnosis
- Diagnosis Date – Diagnosis information
- questionnaire related to sleep studies - Input to Diagnosis and Therapy
- Hospital Data - Input to Diagnosis and Therapy
- Date of Admit - Input to Diagnosis and Therapy
- Date of Discharge - Input to Diagnosis and Therapy
- Primary and Secondary Diagnosis Codes (ICD-10) - Input to Diagnosis and Therapy

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.*

Medical Records Folder File or CHR: The Consolidated Health Record contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. (Department of Veterans Affairs Record Control Schedule RCS 10-1, Chapter Six- Healthcare Records: Health Information Management Service, Code 6000.1, Page III-6-1 (November 2017). Data is stored and archived for 3 years after the last episode of care in Somnoware-e.

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?

The retention has been approved by the National Archives and Records Administration (NARA). The guidance for retention of records is found in the RCS 10-1, and the National Archives and Records Administration. The RCS 10-1 can be found at: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. (Department of Veterans Affairs Record Control Schedule RCS 10-1, Chapter Six- Healthcare Records: Health Information Management Service, Code 6000.1, Page III-6-1 (November 2017). Data is stored and archived for 3 years after the last episode of care in Somnoware-e.

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.

Somnoware-e has a defined data destruction method based on the confidentiality of data. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization and NIST SP 800-88 Rev. 1. Confidential electronic data disposal is done by purging the information and overwriting it beyond state-of-the-art laboratory techniques .Incase data in electronic media containing confidential information has to be disposed, a DBAN (Darik's Boot and Nuke) Tool, Eraser or similar is used to make at least 3 overwrite passes, each with a fixed pattern such as binary zeros with verification after each pass to clean up all confidential information beyond the scope of recovery.

Somnoware-e has a defined data destruction method based on the confidentiality of data. Somnoware-e stores data in electronic form only. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization and NIST SP 800-88 Rev. 1. Confidential electronic data disposal is done by purging the information and overwriting it beyond state-of-the-art laboratory techniques .Incase data in electronic media containing confidential information has to be disposed, a DBAN (Darik's Boot and Nuke) Tool, Eraser or similar is used to make at least 3 overwrite passes, each with a fixed pattern such as binary zeros with verification after each pass to clean up all confidential information beyond the scope of recovery. The retention has been approved by the National Archives and Records Administration (NARA). The guidance for retention of records is found in the RCS 10-1, and the National Archives and Records Administration. The RCS 10-1 can be found at: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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.

Any data used for research, training, or testing in Somnoware-e is de-identified.

All Research proposals are required to be reviewed and approved by the Facility Privacy Officer and Information Security Officer. Only the minimum necessary may be collected and used. Each protocol requires either a HIPAA Waiver, a HIPAA Authorization, or both. In addition, a Limited Data Set may be used only if the affected agencies enter into a Data Use Agreement. All research data collected for use must be in compliance with local policy and VA Handbook 1200.05, Research Activities. This includes testing.

Information used solely for training purposes must not contain patient identification. VHA facilities have test patients (not actual patients) that may be used for the purpose of testing and education. Any presentations that contain information based on patients must be routed through the Facility Privacy Officer to ensure all 18 HIPAA identifiers have been removed.

Also, the HIPAA Safe Harbor Method will be used to eliminate the 18 specific types of data. Additionally, the HIPAA Expert Determination Method will be utilized for any presentations that contain patient information by routing it through the Facility Privacy Officer.

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

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

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: There is a risk that the information contained within Somnoware-e will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed in accordance with the VA Records Control Schedule RCS 10-1. When the retention data is reached for a record, the medical center carefully disposes of the data by the methods described in question 3.4. The Privacy Officer, Information Security Officer, and Chief Information Officer also monitor controls to mitigate any breaches of security and privacy.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Computerized Patient Record System (CPRS) and Cerner electronic health record	For Purpose of the information being shared/received: "Medical Treatment and healthcare services."	Patient demographics including last four of the social security number, International Code of Diseases (ICD)10 codes, (Diagnosis Codes of the patient –the reason why a sleep consult or pulmonary diagnostic study was ordered. This information will be used to stratify the patients if they are not adherent to Positive Airway Pressure (PAP) therapy, Sleep study data.	To CPRS: Existing VA Connected Care Mobile Services- REST Application Programming Interface (API) over Virtual Private Network (VPN) and To Cerner: Health Level Seven (HL7) messages over VPN

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 the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

<u>Mitigation:</u> The security of the information being shared internally must be protected through the use of FIPS 140-2 (or successor) validated encryption implemented according to the specifications in the validated modules certificate. The connections at each end are located within controlled access facilities using physical access devices and/or guards. Individual users will not have access to the data except through the system security software inherent to the operating system. Access is controlled by authentication methods to validate the approved users.

VHA OCC's system and users are expected to protect Iron Bow Technologies partner Somnoware-e system and users are expected to protect VHA OCC in accordance with the Privacy Act and Trade Secrets Act (18 U.S.C. 1905), the Unauthorized Access Act (18 U.S.C. 2701 and 2710), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

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***
ResMed Airview	For Purpose of the information being shared/received: "Medical Treatment and healthcare services." This done to register the device to the patient.	First name, Last name, Patient Unique Identifier and (DOB), Sleep Device Setup date, Patient ResMed patient identifier [if available]. Combination of first name, last name and date of birth	Data Sharing Agreement, Business Agency Agreement (BAA)	HTTPS 443
Phillips EncoreAnywhere	For Purpose of the information being shared/received: "Medical Treatment and healthcare services." This done to register the device to the patient.	First name, Last name, Patient Unique Identifier and DOB Sleep, Device Setup date	Data Sharing Agreement, BAA	HTTPS 443
Twilio	Notification of lack of compliance to therapy	Phone Number, Callback URL, NO PHI	End User License Agreement	HTTPS 443

Sendgrid	Notification of lack of compliance to therapy	To Email ID, NO PHI	End User License Agreement	HTTPS 443
Somnoware-e Commercial Enclave	For Purpose of the information being shared/received: “Medical Treatment and healthcare services.” This is done to enable conducting study community Healthcare Centers	Shared: Patient name, DOB, address, contact information and order Received: Patient Sleep Study Interpretation report, and Sleep Study files	BAA between Somnoware-e and the Community Clinics approved by VA	Sharing via HTTPS 443 Receiving via HTTPS 443 and SFTP 22 (FIPS 140-2)
Watchpat Direct	For Purpose of the information being shared/received: “Medical Treatment and healthcare	Shared: Patient name, DOB Address and Phone number Received: Patient Sleep Study Files	BAA between Somnoware-e and the Watchpat Direct	Sharing via HTTPS 443 Receiving via HTTPS 443 and SFTP 22 (FIPS 140-2)
Northwest Respiratory Services	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Contract between VA medical center and DME ordering companies	Sharing via HTTPS 443 Receiving via HTTPS 443
Calox Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood	Contract between VA medical center and DME ordering companies	Sharing via HTTPS 443 Receiving via HTTPS 443

		Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information		
Mid-Cities Medical	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Contract between VA medical center and DME ordering companies	Sharing via HTTPS 443 Receiving via HTTPS 443

Rotech Healthcare Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Contract between VA medical center and DME ordering companies	Sharing via HTTPS 443 Receiving via HTTPS 443
B & B Medical Services	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Apria Healthcare Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Norco Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

Veteran's Choice	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
SS Medical Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
AeroCare	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Home Care Equipment Inc.	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

Greene Respiratory	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
First Community Care	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Site is their own DME	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Respitec	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

Medics	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Hometown Veterans Medical	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Special Medical Care	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Veterans First Health Care	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

Adapt Health	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Commonwealth Home Health Care	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Trans Ox	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Eagle Home Medical	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

Columbia Ancillary Services	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
CBJ Development	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Apnea Care	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Panakeia	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

MedQuest	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies
Community Surgical Supply	For the purpose of DME order processing by the DME providers associated with VA	Shared: Name, Date of Birth, Last 4 SSN, Address, Email, Cellphone contact, Diagnosis and Oxygen Prescription, Smoking history, Oxygen Titration, Pulse Oximetry, Nicotine Testing, Arterial Blood Gas, Vitals, Sp02 at time of evaluation Received: DME order status, tracking and shipping information	Sharing via HTTPS 443 Receiving via HTTPS 443	Contract between VA medical center and DME ordering companies

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with this system is that external offices/systems could inappropriately use or disclose information, either intentionally or unintentionally.

Mitigation: Iron Bow Technologies partner, Somnoware-e, is responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all their employees relevant to this interconnection. Employee's will be required to security and privacy awareness training as mandated by all applicable contracts. Iron Bow Technologies partner, Somnoware-e, has monitoring and alerting that monitor systems and network 24x7. Alerts are set to notify security personnel when suspicious activity is noted. Somnoware-e has a defined Incident Response process is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders including Breach notification if any, and reduce the likelihood of the incident from reoccurring. Somnoware-e tests its Incident Response Process periodically to keep its Incident Response team abreast of changes to the system and technology.

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.

Personal Information is collected by the VHA facilities. VHA facilities provide notice of information collection in several ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. The Notice of Privacy Practice (NOPP) is then provided to the individual in paper format.

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.

VHA facilities provide notice of information collection in several ways. The initial method of notification is in person during individual interviews or in writing via the

Privacy Act statement on forms and applications completed by the individual. The Notice of Privacy Practice (NOPP) is then provided to the individual in paper format.

Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are:

published in the Federal Register and available online:

- Patient Medical Records-VA, SORN 24VA10A7 (March 22, 2013)
- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10 (Oct. 31, 2012, as amended), 79VA10
- National Patient Databases-VA, SORN 121VA10 (May 11, 2012, as amended)

Please see attached links:

http://www.oprm.va.gov/privacy/systems_of_records.aspx

http://www.rms.oit.va.gov/sor_records.asp

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

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

Yes, individuals do have an opportunity to decline to provide information at any time, however, the VHA may not be able to enroll the Veteran. There is no penalty for declining information. The Notice of Privacy Practices (NOPP) states that the Veteran has the right to request a restriction of the use and disclosure of information; however, under 45 CFR § 164.522(a)(1)(vi) the VHA is not required to agree to such 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.

The VA Care provider obtains the patient consent, and it is recorded in VistA CPRS and/or in Somnoware-e.

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:

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: The privacy risk associated with this system is that the individual will not have prior or existing notice of data collection and uses of information after collection by the source system.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

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.***

VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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)?

No, the system is not exempted from the access provisions of the Privacy Act

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?

VHA Directive 1605.01 Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Under the jurisdiction of VHA, VHA Directive 1605.01 Privacy and Release Information', section 8 states the rights of the Veterans to amend their records. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. 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, or designee.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the quest. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

If the individual discovers that incorrect information was entered into their medical record, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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 the individual accidentally provides incorrect information in their correspondence.

Mitigation: Veterans provide information at the local VAMC. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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?

Access to Somnoware-e FedRAMP environment is granted only based on approval by the CTO or Director of Infrastructure. The system accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every ninety (90) days. Somnoware-e Access control policy requires account termination within twenty-four (24) hours of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination. Physical and environmental security policy. Customers are responsible for managing Somnoware-e application user accounts for their instance of the tool. For an example, customers are responsible for assigning account managers to the Somnoware-e application "Lab manager" and "Centralized Administrator" roles "Lab manager". These roles have privileges to create, modify and delete user accounts. This includes the ability to provision access. It is the responsibility of Somnoware-e customers to ensure access is provisioned in accordance with their own access control policies. The minimum requirements for employees to work in support of this interconnection, to include background investigations and security clearances, will be determined by the contract(s) governing the support services provided by the vendor. Iron Bow Technologies partner Somnoware-e will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all Iron Bow Technologies partner Somnoware-e employees relevant to this interconnection.

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?

Users from other agencies do not have access to the VA instance in Somnoware-e.

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.

Following are the main roles in Somnoware-e application.

i. Lab Manager (Privileged): The facility manager role can view and update all entities under the facility. The role also has privileges to provide access to users.

ii. Lab Technician (Non- Privileged): Can view and update patients assigned to the facility and setup devices and patients for sleep and pulmonary testing.

iii. Physician (Non- Privileged): Can view reports and tracing for patients and studies assigned to them and carry out scoring of studies.

iv. Master Scorer (Non- Privileged): Can view reports and tracing for patients and studies assigned to them and carry out scoring of studies

v. Scorer (Non- Privileged): Can view reports and tracing for patients and studies assigned to them and carry out scoring of studies

vi. Centralized Administrator (Privileged): The Centralized admin role can view and update all entities and facilities user the region. The role also has privileges to provide access to users.

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.

The minimum requirements for employees to work in support of this interconnection, to include background investigations and security clearances, will be determined by the contract(s) governing the support services provided by the vendor. Iron Bow Technologies partner Somnoware-e will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all Iron Bow Technologies partner Somnoware-e employees relevant to this interconnection. All employees, vendors, and contractors are required to follow the Employee Handbook and Acceptable Use Policy. Also, contractors at Somnoware-e are required to sign a HIPAA agreement and a Business Associate Agreement that covers Confidentiality and non-disclosure. Access to third party contractors is granted only after signing these agreements and obtaining a background clearance. The agreements are revisited annually by the Director of HR. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets.

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.

The training and rules of behavior requirements for employees to work in support of this interconnection will be determined by the contract(s) governing the support services provided by the vendor. Iron Bow Technologies partner, Somnoware-e, will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all their employees relevant to this interconnection. All users including employees, trainees, WOCs, volunteers and contractors are required to take annual Privacy, Information Security, and Rules of Behavior Training through the Talent Management System (TMS) course 10176 VA Privacy and Information Security Awareness and Rule of Behavior and 10203 Privacy and HIPAA Focused Training. In addition, 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:* Approved
2. *The System Security Plan Status Date:* October 5, 2020
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* December 17, 2020
5. *The Authorization Termination Date:* December 17, 2023
6. *The Risk Review Completion Date:* December 16, 2020
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include:

Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The system uses cloud and has an agency authorization.

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.*

Software as a Service.

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.

Yes, there is an agreement in place that establish data ownership and it is in accordance to NIST guidance for Federal government data ownership. The VA owns the data.

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.

Yes, there is an agreement in place that establish data ownership and it is in accordance to NIST guidance for Federal government data ownership. The VA owns the data.

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).

Somnoware-e uses AWS Fedramp accredited regions East/West to host its cloud solution. The contract is based on achieving Agency ATO. Only Fedramp accredited cloud services are used within the application. The VA office of Connected Care has a contract in place with Iron Bow / Somnoware-e. The VA has an MOU/ISA in place with Iron

Bow / Somnoware-e, the MOU/ISA has been signed by VA System Owner, Iron Bow ISSO, and Somnoware-e ISSO.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.10.26 13:47:48 -04'00'

Privacy Officer, Dennis Lahl

MATTHEW HESTER Digitally signed by MATTHEW HESTER
Date: 2023.10.26 13:38:58 -05'00'

Information System Security Officer, Matthew Hester

RAY DENNIS Digitally signed by RAY DENNIS
Date: 2023.10.26 15:15:53 -04'00'

Information System Owner, Ray Dennis

APPENDIX A-6.1

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

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

http://www.oprm.va.gov/privacy/systems_of_records.aspx

http://www.rms.oit.va.gov/sor_records.asp

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices