Privacy Impact Assessment for the VA IT System called:

Assessing Social and Community Environments with National Data (ASCEND)

Veterans Health Administration

Rocky Mountain Mental Illness Research Education and Clinical Center

eMASS ID #: 1232

Date PIA submitted for review:

11/3/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michelle Christiano	Michelle.Christiano@va.gov	706-399-7980
Information System Security Officer (ISSO)	Stuart Chase	Stuart.Chase@va.gov	410-340-2018
Information System Owner	Claire Hoffmire	Claire.Hoffmire@va.gov	585-301-1442

Abstract

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

The Assessing Social and Community Environments with National Data (ASCEND) system infrastructure aims to improve suicide-related data collection for the Veteran population as a whole, not only those using VHA services, and will thus obtain data to inform policy and service development and improve the quality of Veteran suicide prevention programs for all Veterans. This system will be used by the foundational ASCEND study and by additional Rocky Mountain MIRECC survey research projects which share a common objective to improve Veteran suicide prevention. The foundational ASCEND study aims to establish a national, recurring survey that can produce valid, population-based estimates of suicidal behavior and correlates among U.S. Veterans. Additional studies which utilize this system may address a wide variety of aims but all share the common objective to improve Veteran suicide prevention.
The ASCEND System collects information for recruitment and sampling frame databases from internal VA entities (i.e., USVETS, VADIR, CDW) that are stored on Rocky Mountain Mental Illness Research Education and Clinical Center (RM MIRECC) secure servers (all behind VA firewalls). These data are also transferred from the RM MIRECC to NORC (ASCEND vendor, not behind VA firewall, on vendor servers/behind vendor firewalls) in accordance with VA & ATO data transfer agreements. These sampling frame and recruitment databases are then used by NORC to invite Veteran and community respondents to participate in survey research studies utilizing the ASCEND system. The ASCEND system uses Voxco, a survey software and data collection tool, to build, administer, collect, and securely store survey responses behind NORC firewalls. Data collection in this system can occur through multiple modes: over the phone (via Computer-Assisted Telephone Interviewing [CATI]); online (via web-based survey application utilizing a compatible internet browser on a desktop, tablet, and/or mobile device), or by paper. Finally, survey data collected within the ASCEND system are returned to the RM MIRECC for secure storage behind VA firewalls.

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?

IT System Name: The Assessing Social and Community Environments with National Data (ASCEND) and Program Office: VA Eastern Colorado Health Care System (ECHCS) Mental Illness Research, Education, and Clinical Center (MIRECC) for Suicide Prevention.

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

The Assessing Social and Community Environments with National Data (ASCEND) system infrastructure aims to improve suicide-related data collection for the Veteran population as a whole, not only those using VHA services, and will thus obtain data to inform policy and service development and improve the quality of Veteran suicide prevention programs for all Veterans. This system will be used by the foundational ASCEND study and by additional Rocky Mountain MIRECC survey research projects which share a common objective to improve Veteran suicide prevention. The foundational ASCEND study aims to establish a national, recurring survey that can produce valid, population-based estimates of suicidal behavior and correlates among U.S. Veterans. Additional studies which utilize this system may address a wide variety of aims but all share the common objective to improve Veteran suicide prevention.

C. Who is the owner or control of the IT system or project?

VA Owned and Controlled/ Non-VA managed and operated.

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?

The expected number of individuals with stored information in the system is 405,000. The typical client or affected individual are U.S. Veterans.

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

In order to meet the aims of ASCEND and related studies and to survey a nationally representative sample of US Veterans, including those who use VHA services as well as those who do not, ASCEND System collects information for recruitment and sampling frame databases from internal VA entities (i.e., USVETS, VADIR, CDW) that are stored on Rocky Mountain Mental Illness Research Education and Clinical Center (RM MIRECC) secure servers (all behind VA firewalls). These sampling frame and recruitment databases are then used by NORC to invite Veteran and community respondents to participate in survey research studies utilizing the ASCEND system. Data gathered from USVETS and VADIR for the sampling frame (e.g., name, address, email, phone number, vital status) will be appended for accuracy and updates from approved third-party vendor sources. This information is required in order to develop accurate and representative sampling frames to invite direct data collection from individuals and to contextualize direct responses collected to ensure that reports or analyses from the ASCEND system are representative of the reporting sample or population. Furthermore, for those who complete study specific surveys, information from those surveys is included. This typically includes information across one or more of the following domains: demographics, military history, physical and mental health, suicidal self-directed violence, healthcare service use and barriers to care, interpersonal relationships, access to lethal means, and community characteristics.

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

Data is transferred from the RM MIRECC to NORC (ASCEND vendor, not behind VA firewall, on vendor servers/behind vendor firewalls) in accordance with VA & ATO data transfer agreements. NORC then uses an approved third-party vendor, through approved VA file transfer via an SFTP portal, to update phone numbers, mailing and email addresses for the sampled Veterans. PressAmerica receives, through secure file transfer, the names, full addresses, study IDs, and PIN numbers for the Veterans in the selected sample and will mail a series of recruitment materials. NORC will use Voxco, a data collection and survey administration platform which is installed on NORC's physical servers, to administer the study survey. This instance of Voxco (and the entirety of the ASCEND system) does not use cloud technology and Voxco (the company) will not receive any ASCEND data. Potential respondents will be able to respond to the survey over the phone, on paper, or online via the mobile, tablet, or desktop internet browser (no application download required). Following the conclusion of ASCEND data collection, the survey response data will remain in the vendor's (i.e., NORC) computing environment for the tasks of data analysis, data merge with community-level data sources, and results reporting. All electronic data will be stored behind NORC's firewall. As requested, and required by the contract, NORC shall submit interim data sets back to the VA following data collection. Transfer of the data set shall be accomplished by a VA-approved mailing option: United Parcel Service (UPS) Ground or United States Postal Service (USPS) Priority Mail for secure delivery service with tracking from pick-up to delivery in accordance with VA Directive 6609 and VA Handbook 6500 to securely mail VA PII data. The ASCEND team will be using the AEGIS Secure Key USB 2.0 (Part Number ASK3-480KB), which is a FIPS 140-2 Validated Removable Storage Device. The device password will be sent separately, via an encrypted VA email. The file will be accessed, and data downloaded immediately upon receipt of the device. Once the sample data has been accessed, the USB device will be re-encrypted and sent back to the VA, where it will be kept in a locked drawer behind locked office drawers.

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?

NORC data centers host the system and are located in Oakbrook, IL and Ashburn, VA. Data disseminated for use in this contract (to include PII and other controlled unclassified information CUI) will reside at more than one site. The VA ISSO team shall maintain security oversight of all data, and system reciprocity will not be observed during mean time periods between VA assessments. Security controls shall remain consistent across sites, and continuous monitoring processes shall be imparted at contractor sites. Any anomaly detected shall be investigated and security incidents will be reported to VA Security Officers immediately. Architectural elements have been submitted and will address security relevant build specks, such that the result of this PIA should not impact either business processes, or technical changes.

3. Legal Authority and SORN

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

The legal authority to operate this project falls under Title 38, United States Code, chapter 73, section 7301. The information collected is contained within the System of Records for VADIR— VA SOR#138VA005Q, as well as within USVETS, which falls under four active SORs: Health Program Evaluation - SOR# 107VA008B; Non-Health Data Analyses and Projections for VA Policy and Planning—SOR# 149VA008A; Veterans, Service Members, Family Members, and VA Beneficiary Survey Records- SOR# 43VA008; and Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA SOR#34VA10.

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?*

This system does not use cloud technology.

4. System Changes

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

None

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

None

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)

Other PII/PHI data elements: the ASCEND system will collect the following information from VA databases (ie: United States Veterans Eligibility Trends and Statistics (USVets) and the VA/DoD Identity Repository (VADIR)) for the purposes of identifying the recruitment sample and completing other key study tasks:

- Transition status
- Maximum separation date
- Veteran status
- VHA usage information
- Years of service
- Retirement indicator
- Branch
- Rank
- Wars served in
- Character of service
- Components served in
- Branch of most recent separation
- Benefits used

In addition, the ASCEND system studies will survey responses related to lifetime history of suicidal ideation and self-directed violence as well as risk and protective factors for these constructs across the social-ecological model for suicide prevention (i.e., individual-, interpersonal-, community-, and societal-level risk factors). Such factors may include but are not limited to constructs such as demographic characteristics, mental health conditions, substance use, trauma history, access to lethal means, experiences with interpersonal relationships, social support and functioning, community environments and problems, and healthcare access, barriers and use.

PII Mapping of Components (Servers/Database)

<**Information System Name**> consists of <**number**> key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <**Information System Name**> and the reasons for the collection of the PII are in the table below.

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

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.

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
Sampling Frame & Recruitment Databases	Yes	Yes	-Social Security Numbers -Full name -Full Address (mailing and/or residential) -Email Address -Telephone Number -Date of Birth -Demographic information (i.e., gender, sex, race, ethnicity) -Military service history (e.g., branch and component of service, periods of service, veteran status, service connection) and applicable dates (e.g., separation dates) -Unique Identifier (e.g., Veteran ID) -Benefits (VBA) and Healthcare (VHA) services	The requested data sets from USVETs and VADIR will be stored on the VA MIRECC Research Data Drive. PII will be used to draw a nationally representative sample of Veterans. The sample data set will be transferred from this location via SFTP or via mail to NORC (for recruitment and data collection). After data collection has ended, interim and final data sets will be transferred back to the MIRECC from NORC.	All PII on the VA MIRECC Research Data drive will be stored behind the VA firewall and will be user-restricted and/or password protected such that only appropriate members of the study team will have access. All PII stored on NORC drives are stored in separate, user-restricted, and password protected folders and

			used and associated dates -Living/vital status indicator -Socioeconomic indicators (e.g., employment status, income) -Competency index/indicators		only appropriate members of the study team will have access.
Survey Response Databases			-Demographic information (i.e., gender, sex, race, ethnicity) -Military service history (e.g., branch and component of service, periods of service, veteran status, service connection) and applicable dates (e.g., separation dates) -Unique Identifier -Benefits (VBA) and Healthcare (VHA) services used and associated dates Socioeconomic indicators (e.g., employment status, income) -Self-reported mental and physical health statuses (including suicidal	Survey data will be used to enhance surveillance of non-fatal suicidal self-directed violence (NF-SSDV; e.g., suicide attempt, suicidal ideation) among Veterans. Through recurring administration (i.e., annually or biannually with different samples), the long-term goal of ASCEND is to track the prevalence and trends over time in NF-SSDV within the broader Veteran population, as well as risk of NF-SSDV among Veterans over time in relation to individual,	TLS 1.2 encryption is used to encrypt data coming in through the survey portal and NORC's storage array uses self-encrypting hard drives to encrypt survey data at rest (AES-256). All PII stored on NORC drives are stored in separate, user-restricted, and password protected folders and only appropriate members of the study

			thoughts and behaviors), substance use, trauma history, access to lethal means, experiences with interpersonal relationships, social support and functioning, community environments and problems, and healthcare access (barriers and use)	interpersonal, and community-level risk and protective factors. Results from these data will be used to inform policy and service development, program evaluation, and quality improvement for Veteran suicide prevention	team will have access.

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?
There are 4 sources of information for the ASCEND system. Two data sets are being used to develop the sampling frame for the ASCEND study:

1. USVETS is a national database of Veterans owned by VA and contains information for over 20 million Veterans. USVETS is produced by the Office of Enterprise Integration: Data, Governance and Analytics.

2. VADIR is the, an electronic repository of active and reserve military personnel, provided to VA by the Department of Defense's Defense Manpower Data Center (DMDC). Data gathered from VADIR and USVets, such as last known vital status, name, address, email address and phone number can change over time and will require updating prior to sample recruitment. Acxiom will be used to append the sample contact information:

3. The approved third-party locating vendor uses its unique databases to confirm and/or update the contact information for the sampled Veterans. Updating mailing addresses, phone numbers and email addresses improves the efficiency of the recruitment process and increases the likelihood that a representative sample of responses will be collected.

4. The ASCEND system creates response data that will be collected directly from the individuals who choose to participate in the survey. Response data will be collected via the Voxco survey administration tool.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information from other sources (e.g., USVETS, VADIR, federally approved vendors) is required in order to develop accurate and representative sampling frames to invite direct data collection from individuals. These additional sources are also used to contextualize direct responses collected to ensure that reports or analyses from the ASCEND system are representative of the reporting sample or population.

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

The ASCEND system itself is a source that will be used and built upon as the system grows.

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?

Using USVETS and VADIR to design sampling frames for projects utilizing the ASCEND system allows the study team to invite participation from members of the entire Veteran population, not just those who use VHA services. It also allows the study team to oversample key groups of Veterans who are known or believed to be at elevated risk for suicide (e.g., those who are females, not utilizing VHA services, recently separated, or rural). Each study utilizing the ASCEND system will seek and obtain approval to use USVETS data through a VA Office of Data Governance & Analytics internal data sharing agreement. Likewise, each study will request VADIR data through the VA Digital Enterprise Service Collaboration Portal. USVETS and VADIR data will be transmitted electronically to study teams in the VA Informatics and Computing Infrastructure (VINCI). To receive contact information updates from an approved third-party locating vendor, NORC must obtain from the VA (via VA approved mailing transfer) a copy of the relevant contact information (including SSN) for only those Veterans included in the selected sample. For mailing, the ASCEND system intends to United Parcel Service (UPS) Ground or United States Postal Service (USPS) Priority Mail for secure delivery service with tracking from pick-up to delivery in accordance with VA Directive 6609 and VA Handbook 6500 to securely mail VA PII data. A AEGIS Secure Key USB 2.0 (Part Number ASK3-480KB), which is a FIPS 140-2 Validated Removable Storage Device will be used for all transfers. The device password will be sent separately, via an encrypted VA email. The file will be accessed, and data downloaded immediately upon receipt of the device. Once the sample data has been accessed, the USB device will be re-encrypted and sent back to the VA, where it will be kept in a locked drawer behind locked office drawers. The transferred file will then be converted into .csv format and uploaded to the approved third-party locating vendor, via an online HTTPS batch portal that uses PGP encryption, directly from NORC's network. The portal reads the submitted file without saving it anywhere. The approved third-party locating vendor then searches its unique databases using a proprietary algorithm that associates information with the person being searched and returns, if available, the best, last seen address and phone number for each sampled participant. Once the batch locating search has finished processing, NORC creates the returns file using the batch portal and

saves it directly to our network. The returns file is never saved by the approved third-party locating vendor, and they do not retain or use any of the data submitted in any way. Voxco, an integrated survey administration and data collection platform, will be used to collect survey responses and will track response rate for targeted Veteran subgroups. Veterans will have three options to respond to the survey: Option 1 - Veterans will access the survey via the URL provided by in the initial mailing. The URL will direct Veteran to a login page and Veteran will log into survey by entering a unique, randomly generated Study ID (e.g., consisting of random combination of characters and numbers that are in no way related to the Veteran's PII [e.g., SSN, DOB, etc.]). Option 2 - Veterans can complete the survey on the phone after receiving a call from NORC or by calling a dedicated phone number. A trained NORC staff member will conduct the survey over the phone. NORC staff will enter survey responses into using Voxco's CATI tool directly. NORC staff will have unique Voxco accounts. Option 3 – Veterans may be mailed a hard copy of the survey instrument. They will have the option to complete the survey using pen and paper, and to mail the survey back to NORC using the included prepaid envelope. NORC will use a subcontractor, Data Shop Inc (DSI), to manually enter the de-identified survey responses from the paper surveys to create an electronic data file. The paper surveys are transferred to DSI on a regular basis. NORC packages the paper surveys into boxes for transfer and they are picked up at the NORC offices by a driver from DSI. After data entry is complete, DSI transfers the de-identified data back to NORC via a SFTP site. The paper surveys are also returned to NORC upon completion. Quality assurance and peer review procedures will be in place to ensure accurate and reliable data entry.

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?

Not applicable; studies utilizing the ASCEND system obtain OMB exemption.

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.

Study sampling frames will be comprised of a current extract of USVETS and an extract from VADIR containing all veterans whose most recent separation is from the start of the previous fiscal year to the present. Efforts will be undertaken to deduplicate USVETS and VADIR records using parallel information available from both data sources. Sampling contact information will be checked for accuracy prior to recruitment through the approved third-party locating vendor; this vendor will append the sampling data to ensure accurate contact information is acquired (i.e., email addresses and phone numbers). Data management procedures will be taken in accordance with ASCEND's Data Management Plan; these procedures include but are not limited to, structure and variable logic checks for variables, a data cleaning program, automated editing rules, and case-level edit logs will be developed. Key demographics such as age, gender, ethnicity, and age will be collected directly from the respondent as part of the research survey and compared to the expected demographic values from the sampling frame. One statistician draws the sample and the other reviews the code and tabular output to verify it aligns with the sample design. Tabular output is shared with the RM MIRECC team. During active data collection, NORC checks the instrument regularly (at least weekly) to ensure that it is working properly; a SAS program will check the number of valid and invalid responses, skips, and breakoffs for each variable in

the survey. NORC reviews the final data file for key data quality indicators such as outliers, non-substantive responses, and completion time. The final dataset is then handed over to the RM MIRECC team.

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 check for accuracy by accessing a commercial aggregator of information.

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

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

The legal authority in this project falls under Title 38, United States Code, Section 730

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: This systems/project has been determined to be of moderate risk, based on its categorization as a "Major" system, without nation security impact. Further, loss of confidentiality, integrity and availability carry financial and reputational damage, without loss to life or limb. Finally, the

negating of research accuracy/effectiveness may suffer in the case of security breach. The system has been classified as a having "Moderate" impact if breached.

Mitigation: In mitigation of moderate risk, the project shall adhere to all applicable security controls and ongoing patching recommendations. These controls include, but are not limited to: NIST, FIPS, STIG and administrative oversight, as assessed and directed by appointed VA Security Officers. Any residual risk found within the solution shall be tracked via POA&M and security relevant changes will be recorded in eMASS. System administrators, engineers and developers shall report security relevant changes and/or issues to the NORC Security Team immediately. The NORC Security Team will notify the NORC VA ASCEND system teams. All site logging and auditing standards shall be met, to include scanning, eradication effort and re-scan (until risk has been removed). All high/zero-day risk shall be addressed immediately, and all else addressed as part of in place patch management processes. FIPS approved encryption shall be used in protection of all CUI data, to ensure its protection in travel and at rest. Finally, all accesses shall begin with an explicit deny all-to-all and allowed only upon verified need and authorization. All additional mitigation requirements shall be governed by on-site, VA NSOC and VA security professionals.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not used
SSN	Used as a patient identifier	Not used
Full address	Used to contact the individual	Not used
Email address	Used to contact the individual	Not used
Telephone number	Used to contact the individual	Not used
Date of Birth	Used to identify patient age and confirm patient identity	Not used
Demographic information	Used to create sampling frame	Not used
Military service history	Used to create sampling frame	Not used
Transition status	Used to create sampling frame	Not used
Maximum separation date	Used to create sampling frame	Not used
Veteran status	Used to create sampling frame	Not used
Years of service	Used to create sampling frame	Not used
Retirement indicator	Used to create sampling frame	Not used
Branch/Branch of most recent separation	Used to create sampling frame	Not used

Rank	Used to create sampling frame	Not used
Wars served in	Used to create sampling frame	Not used
Character of service	Used to create sampling frame	Not used
Components served in	Used to create sampling frame	Not used
Unique identifier	Used to confirm patient identity	Not used
VA Benefits and Healthcare services used	Used to create sampling frame	Not used
Living/vital status indicators	Used to create sampling frame	Not used
Competency index/indicators	Used to create sampling frame	Not used
Self-reported mental and physical health statuses	Used to achieve study aims	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?

Statistical analysis software will be used to analyze the data collected from studies utilizing the ASCEND system. Survey data may be merged with complementary clinical and non-clinical, individual-level and publicly available community-level datasets, for further analysis. However, survey data will not be entered into an individual's existing medical record and will not be accessible to Government employees who make determinations about that individual.

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.

In the event that a study team member has an interaction with a research participant that incidentally reveals that the individual is in distress or thinking of harming themselves or others, the study team will refer that individual to the appropriate emergency or crisis resource. Outside of these safety procedures, no action would be taken against or for an individual because of the data generated from studies utilizing the ASCEND system.

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?

The system utilizes TLS 1.2 encryption to encrypt survey data in transit. NORC's storage array uses self-encrypting hard drives to encrypt data at rest (AES-256). All primary arrays use FIPS 140-2 compliant cryptographic modules for key generation, hashing, and random number generation. When data is transferred from NORC to RM MIRECC, we will be using the AEGIS Secure Key USB 2.0 (PartNumber ASK3-480KB), which is a FIPS 140-2 Validated Removable Storage Device. The device password will be sent separately, via an encrypted VA email.

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

SSNs are only used for contact information in the sample. They are not collected as part of the survey. They are not stored in the Voxco system. The files containing the SSNs are stored on NORC's secure file system. Only Project staff with approved access are allowed to access the file.

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

NORC applies the appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

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.

All employees with access to system information will undergo a background check and security/privacy training prior to beginning work duties. Data in transit shall be protected each security boundary by firewalls, and all rulesets shall begin with an explicit deny all-to-all and only allow traffic that with verified need and authorization. To ensure protection against privacy breach, data in use shall only be used by fully security trained individuals, with a role-based account to access such data, and a well-defined business requirement to take action involving the data. Access to those with a need-to-know (least privilege) requirement to the data will be granted by supervisors, and the VA ASCEND Principal Investigators will have oversight of new user access requests. All user rights must be approved by the Project Director or delegate prior to access being granted. Managers are required to submit a user deactivation request for anyone removed from the project so that data access will be removed immediately. All data use and storage (system audit logs) shall be continuously monitored, such that any

anomalies are spotted and addressed quickly, by security engineers. Data in transit shall be protected each security boundary by firewalls, and all rulesets shall begin with an explicit deny all-to-all and only allow traffic that with verified need and authorization.

2.4a How is access to the PII determined?

Access to those with a need-to-know (least privilege) requirement to the data will be granted by supervisors, and the VA ISSO team, who will have oversight of new user access requests. All user rights must be approved by the Project Director or delegate prior to access being granted.

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

NORC IT SOP AC-2 Account Management and AC-3 Access Enforcement provide document controls and procedures for access.

2.4c Does access require manager approval?

Yes.

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

All data use and storage (system audit logs) is continuously monitored., such that any anomalies are spotted and addressed quickly, by NORC security engineers.

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

Responsibility for the safeguarding of PII is provided by the VA and NORC Information System Security Officers (ISSOs).

Section 3. Retention of Information

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

3.1 What information is retained?

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

The following data elements/items will be retained within the ASCEND authorization boundary during the duration of survey and approved ATO determination.

- First, middle and last name
- Veteran ID (SSN)
- Indicator for whether person was living at the end of the most recent FY available
- Full address
- State name
- County name of residence
- Urbanicity (urban/rural)
- Urbanicity (urban/large rural/small rural/isolated)
- Telephone number
- Email address
- Date of birth

• Gender
• Ethnicity
• Race
• Transition status
• Maximum separation date
• Veteran status
• VHA usage information
• Years of service
• Retirement indicator
• Branch
• Rank
• Wars served in
• Character of service
• Components served in
• Branch of most recent separation
• Benefits used
• ASCEND survey response data

Study data will be maintained and destroyed in accordance with VA Records Control Schedule 10-1 and the VA Eastern Colorado Health Care System (ECHCS) Research Investigator Files Retention and Disposition Standard Operating Procedures.

Information created and/or received by NORC as part of the ASCEND contract will be returned to the VA or destroy at the completion of the contract. No such information will be retained by NORC unless retention is required by law or specifically permitted by the VA.

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.*

Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. The VA Office of Policy and Planning (OPP) will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, "electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules." All VA data will be handled as documented within associated security documents. Shared data will be returned to

the VA once it is no longer needed for research purposes, when the system ATO expires, and/or at the conclusion of the research study. Regarding media to be mailed to NORC, the data retention and media return process is detailed below. Data mailed to NORC is a copy of data that will remain held by the VA, and the below information does not apply to that original data. Mailed Data Receipt and Return Upon receiving media via mail, the recipient will notify the sender of receipt and open the file with the provided password. The recipient will return the media using the same mailing protocol within five (5) business days. USB device will be re-encrypted before return to the VA. Data/Media Storage Upon receiving the media device and when extend time is required to return the device back to VA possession, the authorized recipient(s) will securely store the device when not in use. Extend time consists of when the device is stored overnight, one day or more, and not in use, and will not exceed more than 5 business days. Additionally, the media device will not be out of sight/possession of the authorized recipient(s) during use. Authorized personnel from listed companies in the signed Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) document for the ASCEND information system will securely store the device in a lockable cabinet/drawer and will always keep the office/room locked when the device is not in use. The listed security measurements are in accordance with VA Handbook 6500 security control Media Storage (MP-4)

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.

The ASCEND information system is not the system of records for the associated data. At no time are records being destroyed. Official approval is not required. Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. OPP will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, ‘‘electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.” NORC retention schedule for agency systems uses the following from the NARA-approved disposition authority table. Disposition: N01-0064-1987-0001, Item 119-2 / Record Category: 146 Research and Evaluation Technical Report Files 146-2. Destroy when no longer needed for reference.

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

NORC sanitizes non-encrypted system media prior to disposal, release out of NORC control, or release for reuse. NORC utilizes sanitization mechanisms in alignment with NIST Special Publication 800-88.

rcs10-1.pdf (va.gov)

NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization | NIST

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

Upon completion of the project, NORC will deliver, destroy or sanitize any electronic or paper records as outlined by the Department of Veterans Affairs (VA) system business owner/information systems owner, including those that contain PII and PHI data. Clear documentation, signed by the NORC Information Technology Security Officer, will accompany the tasks maintaining a record of the data that is sanitized or destroyed. If the project requires any archiving of data, NORC will work with the VA to determine the specific data to be archived, length of time, storage, purpose, security, and other requirements necessary to ensure that all needs are met. NORC will not dispose of any records unless authorized by the VA.

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.

SPI will be stored electronically by NORC (Contractor) for the duration of the ASCEND system. Once final data sets have been delivered to the VA and the contract tasks have been completed, electronic data will be destroyed by NORC and its subcontractors in accordance with the contract deliverable data destruction plan. The final data set records contained in this system are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. OPP will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, ‘‘electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.”

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.

Protections will be put into place to maintain the confidentiality of records and reduce risks to privacy. All electronic data will be stored in strict compliance with Colorado Multiple Institutional Review Board (COMIRB) and VA R&D standards. Specifically, electronic data will be stored behind the VA firewall in a VA shared drive or other VA system that maintains compliance with all VA security polices and regulations. Access to all electronic study files will be password protected and/or user-restricted to key study personnel. As a research system, ASCEND minimizes the use of PII wherever possible, throughout project tasks. NORC sampling specialists will assign study ID numbers to the selected sample once it has been drawn, and research participants will be identified only by this anonymous study ID wherever possible.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information could be retained for longer than necessary which could result in the information being compromised or incorrectly disposed of.

Mitigation: The records contained in this system have not been scheduled and will be kept indefinitely until such time as they are. The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States.

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***
Office of Data Governance and Analysis (DGA) – United States Veterans Eligibility Trends and Statistics (USVETS)	Requested data will be used as a sampling frame with which to draw a representative sample of Veterans to survey for projects utilizing the ASCEND system.	• *Social Security Numbers* • *Full name* • *Full Address (mailing and/or residential)* • *Telephone Number* • *Date of Birth* • *Demographic information (i.e., gender, sex, race, ethnicity)* • *Military service history (e.g., branch and component of service, periods of service, veteran status) and applicable dates (e.g., separation dates)* • *Unique Identifier (e.g., Veteran ID)* • *Benefits (VBA) and Healthcare (VHA) services used and associated dates*	Access to USVETS data on the VA SAS Grid and/or in VINCI is granted by the VA Office of Data Governance & Analytics (DGA) following VA Data Sharing Agreement approval. USVETS Data (va.gov)

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***
		• *Living/vital status indicator* • *Socioeconomic indicators (e.g., employment status, income)* • *Competency index/indicators*	
Department of Defense's Defense - Manpower Data Center (DMDC) – VA/DoD Identity Repository (VADIR)	VADIR will be used as a supplement to the USVETS sampling frame, specifically to identify Veterans who have been recently discharged between the time of the last USVETS update and the date of the data request.	• *Social Security Numbers* • *Full name* • *Full Address (mailing and/or residential)* • *Email Address* • *Telephone Number* • *Date of Birth* • *Demographic information (i.e., gender, sex, race, ethnicity)* • *Military service history (e.g., branch and component of service, periods of service, veteran status, service connection) and applicable dates (e.g., separation dates)* • *Unique Identifier (e.g., Veteran ID)* • *Living/vital status indicator* • *Socioeconomic indicators (e.g., employment status, income)*	RM MIRECC study teams utilizing the ASCEND system will request VADIR data through the VA Digital Enterprise Service Collaboration Portal. VADIR data will be transmitted electronically to the appropriate RM MIRECC study team in via encrypted email or secure transfer on Microsoft Teams.
Business Intelligence Service Line (BISL) -	The Death Ascertainment File in the CDW will be used to confirm	• *Social Security Numbers* • *Full name*	RM MIRECC study teams utilizing the ASCEND system will request CDW

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***
Corporate Data Warehouse (CDW)	whether sampled Veterans are alive. Data from CDW may also be used to confirm whether Veterans in the sampling frame are VHA service users and to obtain additional information (i.e., diagnoses, types of service use) for respondents who have used VHA services.	• *Full Address (mailing and/or residential)* • *Email Address* • *Telephone Number* • *Date of Birth* • *Demographic information (i.e., gender, sex, race, ethnicity)* • *Military service history (e.g., branch and component of service, periods of service, veteran status, service connection)* • *Unique Identifier (e.g., Veteran ID)* • *Benefits and VHA services used and associated dates* • *Living/vital status indicator* • *Socioeconomic indicators (e.g., employment status, income)* • *Competency index/indicators* *1.*	data through the Data Access Request Tracker (DART) Research Request Process. Once access has been approved, data is made available to the appropriate RM MIRECC study team in a study specific SQL Server database.

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 data could be shared with VA users who do not have a need-to-know-requirement to access the data.

Mitigation: Data shall only be accessible by VA employees/WOCs that have a roll-based requirement to access data for research purposes. Protections will be put in place to maintain the confidentiality of records and reduce risks to privacy. All electronic data will be stored in strict compliance with Colorado Multiple Institutional Review Board (COMIRB) and VA R&D standards. Specifically, electronic data will be stored behind the VA firewall in a VA shared drive or in another system that maintains compliance with all VA security polices and regulations. Access to all electronic study files will be password protected and/or user-restricted to key study personnel. As needed, the study PI (Claire Hoffmire) will consult with the VA ECHCS Privacy Officer and Information Security Officer through VA R&D on data security matters. All study personnel will meet human subject's protection and other training requirements, per COMIRB approval, as well as secondary approval from the local VA R&D.

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***
Voxco (NORC)	NORC will receive the ASCEND sample to conduct recruitment and data collection. NORC will also mail incentives to Veterans	Full data set: controlled unclassified information	DUA	Via USB drive in mail. VA encrypted device.
Lexis Nexis	NORC will use a VA-approved locating vendor to update Veteran contact information for the purposes of recruiting more efficiently.	Full name, SSN, mailing address, phone number, DOB	None	NORC creates a file with limited sample information (name, address, phone number, email, SSN) and upload it to a secure LexisNexis online HTTPS batch portal that uses PGP encryption, which NORC has a specific password-protected

				account for. The LexisNexis system would then read our submitted file and process the contact info append within that file and without saving it anywhere on their end. Once the batch append has finished processing, NORC downloads the updated file to their secured network. NORC would then delete the file in the LexisNexis portal and LexisNexis will no longer have access to it as they never download it from the portal and do not retain or use any of the data that we submit in any way.
PressAmerica	PressAmerica will mail recruitment materials	Full name, mailing address, study ID	DUA, NDA	Secure Web-Portal
NORC Technical Support Desk	The NORC Respondent Care Center	Full name, current location, email address, phone number, study ID	BAA	All PII stored on NORC drives are

(i.e. NORC Respondent Care Center Team) (NORC)	Team may collect information from incoming calls or emails for safety purposes.			stored in separate, user-restricted, and password protected folders and only appropriate members of the study and Respondent Care team will have access. De-identified encrypted safety logs may be shared with MIRECC/VA as needed to provide safety responses.

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: There is a moderate risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: All shared PII shall be authorized for release, as governed by project management, for the purpose of use in identifying most current contact information for study subjects. All logging and auditing shall be:
• Reviewed daily, for errors, inconsistency and anomalies
• Limit in viewers (for audit trails) to those with a job-related need and current privileged access
• User access control and authentication is discussed in section 8.1
• Protected from unauthorized modifications
• Promptly backed-up to a centralized log server or media that is difficult to alter
• Subject to file integrity monitoring/change detection software, to ensure that existing log data cannot be changed without generating alerts (although new data being added must not cause an alert)

Data Mailing
In accordance with VA Directive 6609 and VA Handbook 6500, the electronic media (e.g. thumb drive) containing VA PII data will be secured with a password that is sent to the recipient in a separate email. The data will be mailed with a tracking service. A notice sheet containing language that explains that there are penalties for violations of the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule will accompany the mailing. The sender will also notify the recipient via email that the package is underway.

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.

Applicable authority for ASCEND is under the following SOR's - Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA'' (138VA005Q), Health Program Evaluation SOR# 107VA008B; Non-Health Data Analyses and Projections for VA Policy and Planning SOR # 149VA008A; Veterans, Service Members, Family Members, and VA Beneficiary Survey Records SOR # 43VA008; and Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA SOR#34VA10. In addition, recruitment letters and consent information inform Veterans of their right to consent to participate in the study or decline to provide information.

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

Not Applicable

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.

This is an optional survey. All information collected by the ASCEND system is received by willing survey participants.

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.

Invited Veterans may decline to participate in ASCEND at any time by calling or emailing the study help desk. Recruitment letters will include a consent postcard that clearly explains voluntary participation and the Veteran's right to decline to provide information. The decision whether or not to participate will have no effect on the Veterans access to benefits, current or future clinical care.

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

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

Individuals consent only to the use of their information for research purposes. There are no other uses of the ASCEND information.

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals will be unaware that their information was contained in the sampling frame databases.

Mitigation: Individuals consent only to the use of their information for research purposes. There are no other uses of the ASCEND information. Notice was given to the general public in the Federal Register on the following SORNs: Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA'' (138VA005Q) – 12/23/2022, Health Program Evaluation SOR# 107VA008B 1/25/2021; Non-Health Data Analyses and Projections for VA Policy and Planning SOR # 149VA008A 1/25/2021; Veterans, Service Members, Family Members, and VA Beneficiary Survey Records SOR # 43VA008 1/25/2021; and Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA SOR#34VA10 6/23/2021.

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.

As this is a research project, there is no process for access, redress and correction of an individual's record. Data collection for this survey is a one-time process. While a participant is in the process of completing a survey (either over the phone, on the web, or using a pen and paper), he/she may change the answers to his/her survey, but once a survey is submitted, the survey is locked, and the participant may not revisit the survey, or the information submitted.

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.***

Not applicable

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)?

Not applicable

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?

Not applicable

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.

As this is a research project, there is no process for access, redress and correction of an individual's record. Data collection for this survey is a one-time process. Veterans will not be able to edit their answer choices once they have completed the survey.

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.

Survey data may not be corrected by participant after submission.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans will not be able to edit their answer choices once they have completed the survey.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Privacy Risk: As this is a research project, there is no process for access, redress and correction of an individual's record.

Mitigation: Information gathered will not be used to identify any specific Veterans. Survey responses will be used for research purposes only and will not impact clinical care or eligibility for any community or VA services.

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 the ASCEND system on NORC networks requires the individual to submit a ServiceNow access request. Access to those with a need-to-know (least privilege) requirement to the data will be granted by NORC Supervisor. The VA ASCEND provides oversight of new user access requests.

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?

No users from other agencies. VA ISSO team establishes the criteria for what PII can be shared from the VA ASCEND system.

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.

There are five types of users for the ASCEND system:
1.Invited participants - Veterans may log on to complete the ASCEND survey by visiting a public-facing website and entering their Study PIN number. The Veteran will have "write-only" access to the system and will not have access to any PII within the ASCEND system.

2.Technical support staff – will have "write-only" access to the ASCEND system, through the public-facing website, to enter data from returned paper surveys. Technical support staff will also have access to PII (email address, name, current location) as provided by Veterans who call or email the support desk.

3.NORC Interviewers/Operators and Managers – Call Center Interviewers/Operators perform phone-based interviews with respondents. Each case to be worked is added to the Interviewer/Operator case load once his/her workstation appears as available (i.e. technical security controls built into the software

prevent interviewers/operators from selecting which case[s] they prefer to work on). Call Center Managers review cases to assure quality and accuracy, but do NOT interact with respondents (except to manage customer service
incidents/issues).

a. Call Center Interviewer/Operator
    i. Secure card key access to area
    ii. User ID (Active Directory)
    iii. Password
    iv. Upon acceptance the password/passphrase, the VOXCO system returns an authentication code via telephony, which must be entered at prompt to complete authentication
b. Call Center Case Managers
    i. Working from within the manned/secured call station:
        1. Secure card key access to area
        2. User ID (Active Directory)
        3. Password
    ii. Working from a managed external workstation (managed, patched and updated by NORC):
        1. VPN access (via hardware certificate)
        2. User ID (Active Directory)
        3. Password
        4. Authentication code (sent to mobile device and entered into the system)
        5. Re-enter User ID (Active Directory)
        6. Re-Enter Password

4. NORC Statisticians – have access to the ASCEND system, working from a managed external workstation (managed, patched and updated by NORC):

i. VPN access (via hardware certificate)
ii. User ID (Active Directory)
iii. Password
iv. Authentication code (sent to mobile device and entered into the system)
v. Re-enter User ID (Active Directory)
vi. Re-Enter Password

In addition, these users have access to the ASCEND data set on the VA network, through WOC appointments obtained in 2009 through the VA ECHCS MIRECC. When accessing the VA network though Citrix using PIV authentication, NORC statisticians act as VA users (user type #5, listed below).

Lastly, NORC statisticians access sample data mailed via USB removable drive for the purposes of transferring the data from the USB drive to the NORC secure server. They will be permitted to receive, open, decrypt, and return the removeable media. They will decrypt the removable media using a password securely emailed to their VA email address, which is accessed via PIV authentication.

5. VA Users – Once the ASCEND data set has been returned to the VA (following data collection and analysis), the data will live on the VA Rocky Mountain MIRECC research data drive where it can be accessed by VA users, who have access to the file folder where it is shared, using PIV authentication.

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 ASCEND system will collect and maintain confidential personal data, the protection and security of which is fundamental to the project. NORC holds a BAA with the VA for the relevant contract and implements extensive security measures to protect all aspects of computer and data security through a multi-tiered approach of access control and monitoring, data encryption during transmission, and continuous upgrades of plans and policies to align with the changing environment.

All data containing respondent PII will be stored in a restricted directory following the least- privilege access model. All survey data is collected using unique de-identified keys and cannot be merged with any other VA administrative or medical records without a crosswalk. Any necessary crosswalks between individual-level data sources (e.g. VA administrative or health records) will be developed within the restricted environment and assigned unique de-identified keys to allow for linkage without the use of PII. Merging of community-level datasets are generally conducted at a geographic or otherwise aggregated level and typically are managed at the de-identified level.

Information provided above is directly taken the Confidentiality and Data Security Plan received September 2023. This document was one of the required documents for our latest contract executed as of August 2023. Contract renewals are variable based on the funding period per project and government funder.

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.

NORC CATI interviewers complete the following training modules: NORC code of ethics, data security and data integrity, confidentiality, privacy and HIPAA. Call center staff complete the following training modules: Attestation/Acknowledgement of terms within Data Use Agreements, Data classifications and classified data handling (including HIPAA training), Employee Codes of Conduct, Privileged Access Agreements, Identifying and Reporting Cyber Incidents, Annual Security Refresher Briefing. In addition, ASCEND VA users and users with access to the VA site-to-site VPN connection will complete OI&T security and privacy awareness training on a yearly basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* August 2, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* October 28, 2022
5. *The Authorization Termination Date:* October 27, 2024
6. *The Risk Review Completion Date:* January 4, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* C - Moderate, I - Moderate, A - Low; Impact - 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.***

Section 9 – Technology Usage

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

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

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

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

No, the system does not use cloud technology.

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

Not applicable. The system does not use cloud technology.

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in

the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

Not applicable. The system does not use cloud technology.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?
What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Not applicable. The system does not use cloud technology.

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

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

ID	Privacy Controls
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.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2024.01.17 17:06:31 -05'00'

Privacy Officer,

STUART CHASE

Digitally signed by STUART CHASE
Date: 2024.01.18 07:32:02 -05'00'

Information System Security Officer,

CLAIRE HOFFMIRE

Digitally signed by CLAIRE HOFFMIRE
Date: 2024.01.18 15:15:42 -05'00'

Information System Owner,

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).

VADIR and USVets each have applicable system of record notices. 1) Veteran, Patient, Employee, and Volunteer Research and Development Project Records SOR# 34VA10; 2) VA Health Program Evaluation; SOR# 107VA008B; 3) Non-Health Data Analyses and Projections for VA Policy and Planning—SOR# 149VA008A; 4) Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - SOR# 43VA008; 5) Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA'' (138VA005Q).

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