Privacy Impact Assessment for the VA IT System called:

Operation Cloudy

National Center for Collaborative Healthcare Innovation (NCCHI)

Date PIA submitted for review:

03/03/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Andrea Wilson*	*Andrea.Wilson3@va.gov*	*321-205-4305*
Information System Security Officer	*Roland Parten*	*Roland.Parten@va.gov*	*205-534-6179*
Information System Owner	*Angela Gant-Curtis*	*Angela.Gant-Curtis@va.gov*	*540-760-7222*

Abstract

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

The Veterans Health Administration (VHA) Innovations Ecosystem (IE) will be utilizing the Visión machine learning platform, planned to be hosted in the VA Enterprise Cloud (VAEC) Amazon Web Service (AWS) segment of the network, behind the VA firewall. The system is a healthcare data science as a service (managed service) for the purpose of analysis and auditing of the COVID-19 vaccine rollout across the VA Health Care System. The system will utilize data from the VHA Corporate Data Warehouse (CDW). Using validated machine learning algorithms, we can identify Covid-19 Vulnerable Individuals and, Pathways for Optimizing Outreach and Vaccination activities.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

Operation Cloudy is a project being facilitated by the National Center for Collaborative Healthcare Innovation (NCCHI) under the guidance of the Veterans Health Administration (VHA) Innovations Ecosystem (IE). The system will utilize the Visión machine learning platform, planned to be hosted in the VA Enterprise Cloud (VAEC) Amazon Web Service (AWS) environment. The system is a healthcare data science as a service (managed service) for the purpose of analysis and auditing of the COVID-19 vaccine rollout across the VA Health Care System. The system will utilize data from the VHA Corporate Data Warehouse (CDW). Using validated machine learning algorithms, we can identify Covid-19 Vulnerable Individuals and, Pathways for Optimizing Outreach and Vaccination activities.

During the pilot we will score 1.5 M active beneficiaries (census and 18- months of claims data). Then following the initial phase, to score the balance of the active beneficiary population for a total of 6M active beneficiaries (4.5M active beneficiaries incremental to pilot). The data will not be shared outside of the VA and the final dashboard work bench will be stripped of all PHI information.

Once hosted in the VA EC (Enterprise Cloud) environment all VA stakeholders will be able to utilize the workbench dashboard. The Data science platform is currently completing the processes to obtain an ATO within the VAEC. Authority to operate: Title 38 of U.S. Code section 201. The change in the business process will be that VA Stakeholders will be able to use the workbench dashboard portal to identify Covid-19 Vulnerable Individuals and prioritize Pathways for Optimizing Outreach and Vaccination activities.

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.

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 Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Other Unique Identifying Number (list below)

1. Claim ID
2. Original claim id (for adjusted or rebilled/corrected claims)
3. Member ID
4. Subscriber ID
5. Line of business (such as Medicare Advantage, ACA, Commercial, ASO, etc.), with ID and description
6. Service from and to dates
7. Servicing provider ID and NPI
8. Billing provider ID and NPI
9. Admitting diagnosis and version (ICD 9 v ICD 10)
10. Primary diagnosis and version (ICD 9 v ICD 10)
11. All other diagnosis codes (2-25) (facility claims)
12. All procedure codes and ICD-10-PC (1-25) (facility claims)
13. DRG code
14. Bill type (4-digit code)
15. Claim status (accepted, pending, adjusted, etc.)
16. Claim ID R
17. Claim line number
18. Claim line service from and to dates
19. Servicing provider ID and NPI
20. Billing provider ID and NPI
21. Place of service
22. Diagnosis codes (full set) and version (ICD 9 v ICD 10)

23. Procedure codes (full set)
24. Modifiers (1-4, or more, if available)
25. Type of service code (professional claims)
26. Revenue codes (facility claims)
27. Claim line status (paid, pending, adjusted, denied)
28. Member ID
29. Subscriber ID
30. Unique individual identifier
31. Member physical address
32. Member zipcode
33. Member preferred language
34. Member date of birth
35. Member gender
36. Member date of death (if applicable)
37. Effective dates
38. Termination dates (eligibility history)
39. Family relationship to subscriber ID
40. PCP Provider ID
41. Provider ID
42. Provider NPI

PII Mapping of Components

Operation Cloudy consists of 4 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Operation Cloudy and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
[VHACDWA01.vha.med.va.gov] Linux data Processing Host (r5.large)	**Yes**	**No**	Claim ID, Original claim id (for adjusted or rebilled/corrected claims), Member ID, Subscriber ID, Line of business (such as Medicare Advantage, ACA,	**PII required for base functionality of analysis based on clinical factors, social determinants of health (SDOH)**	**FedRamp approved VAEC AWS platform. FIPS 140-2 Compliance. VA 2FA NEMA Login.**

			Commercial, ASO, etc.), with ID and description, Service from and to dates, Servicing provider ID and NPI, Billing provider ID and NPI, Admitting diagnosis and version (ICD 9 v ICD 10), Primary diagnosis and version (ICD 9 v ICD 10), All other diagnosis codes (2-25) (facility claims), All procedure codes and ICD-10-PC (1-25) (facility claims), DRG code, Bill type (4-digit code), Claim status (accepted, pending, adjusted, etc.), Claim ID, Claim line number, Claim line service from and to dates, Servicing provider ID and NPI, Billing provider ID and NPI, Place of service, Diagnosis codes (full set) and version (ICD 9 v ICD 10), Procedure codes (full set), Modifiers (1-4,	**factors and the standard visualization and reporting functions of the application.**	

			or more, if available), Type of service code (professional claims), Revenue codes (facility claims), Claim line status (paid, pending, adjusted, denied), Member ID, Subscriber ID, Unique individual identifier, Member physical address, Member zipcode, Member preferred language, Member date of birth, Member gender, Member date of death (if applicable), Effective dates, Termination dates (eligibility history), Family relationship to subscriber ID, PCP Provider ID, Provider ID, Provider NPI		
[VHACDWA01.vha.med.va.gov] AWS S3 Storage	**Yes**	**Yes**	**Same data as listed above**	**PII required for base functionality of analysis based on clinical factors, social determinants of health (SDOH) factors and the standard visualization**	**FedRamp approved VAEC AWS platform. FIPS 140-2 Compliance. VA 2FA NEMA Login.**

				and reporting functions of the application.	
[VHACDWA01.vha.med.va.gov] Redshift (dc2.8xl)	Yes	No	Same data as listed above	PII required for base functionality of analysis based on clinical factors, social determinants of health (SDOH) factors and the standard visualization and reporting functions of the application.	FedRamp approved VAEC AWS platform. FIPS 140-2 Compliance. VA 2FA NEMA Login.
[VHACDWA01.vha.med.va.gov] Analytics Linux	Yes	Yes	Same data as listed above	PII required for base functionality of analysis based on clinical factors, social determinants of health (SDOH) factors and the standard visualization and reporting functions of the application.	FedRamp approved VAEC AWS platform. FIPS 140-2 Compliance. VA 2FA NEMA Login.

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The system will utilize data from the VHA Corporate Data Warehouse (CDW). Patient claims data and electronic health record (HER) data is already aggregated in the CDW, providing as single source of data for the required analysis. The collected data will then be stored in the VAEC AWS environment.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected from the Corporate Data Warehouse (CDW) using a Structured Query Language (SQL) to identify the needed records and provide an output of data required into a database table. The data would then be transferred into the AWS Cloud Server via Secure Sockets Layer (SSL) protocol connection for analysis.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the *system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.*

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

The data collected is for the purpose of analysis and auditing of the COVID-19 vaccine rollout across the VA Health Care System. We will identify Covid-19 Vulnerable Individuals and, Pathways for Optimizing Outreach and Vaccination activities. The data output will be provided on a dashboard for clinicians, stripped of PHI and PII information. The ability to risk stratify veterans for the vaccine is imperative to the VA Mission.

1.5 How will the information be checked for accuracy? How often will it be checked?

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Data sources inputted into the machine learning platform will be authoritative sources of data. Data will be validated with informatics team to confirm no data corruption in submission. Further data validation will be completed as part of the set-up of the platform, as outlined by the contract deliverables.

(Below are specific task and deliverables)
Task 1. Subcontract and reporting
Cogitativo will provide weekly updates to VHA IE on progress.

Task 2. Project work plan, kickoff, and meetings
Prepare a draft project work plan for review at kickoff meeting with final acceptance approval by VHA IE. The project kickoff meeting will be held after the subcontract has been signed. The project kickoff will review the project work plan tasks and schedule. Project meetings with VHA IE will occur on a weekly basis (or as needed) until project deliverables and presentation(s) are completed or end of pilot project period. Provide post-meeting summaries to VHA IE.

Task 3. Inventory claims data from VHA

VHA IE to provide the enrollment and claims data for at least the following coverage levels: 1.5 million beneficiaries. The time period for the paid claims data will be calendar 2019 and available 2020 data.

Deliverable: Email notification of final Pilot Beneficiary enrollment count to VHA IE.

Task 4. Risk Scoring
Analyze and aggregate risk scores of hospitalizations post-COVID-19 infection, using scoring algorithms and inputs on demographics, social determinants, health conditions, clinical diagnoses, and care services. The scoring for COVID-19 hospitalization risk will be categorized into high, medium, and low-risk groups. Risk scores will be expressed as odds ratios for groups identified and probability bins of hospitalizations post COVID-19 infection.

Deliverable: Tableau visualization and summary tables on risk scores (high, medium, and low), in CSV format, for individual categories by age, sex, race, health conditions, and social determinants by coverage level and geographic areas including 5-digit zip code and county, excluding identifiable PII and PHI. Identify attributed primary caregivers and KCLs for high and medium risk individuals. Deliver to VHA Innovation Ecosystem leads.
Proprietary and confidential 4

Task 5. Draft report on Risk Scoring & Ranking
Prepare a draft report on risk score and ranking findings describing the data sources, methodology, and relative risk of different state-level populations geographic area. Output tables and Tableau Workbook from Task 4 will be included in the draft Quarterly report. The summary will include documentation of machine learning methods used in the preparation of analyses in the draft report and will be provided to VHA IE.

Deliverable: Draft Report and Tableau Visualization incorporating findings from Task 4 will be delivered to VHA IE lead. Note: Recipient will need to have Tableau Reader version 2020.3.2 for report visualization.

Task 6. Final report on Risk Scoring
Prepare final Quarterly report evaluating the findings of the machine learning algorithms incorporating VHA IE comments from the draft report submitted under Task 5.

Deliverable: Final Quarterly Report. Deliver to VHA IE leads. Note, recipient will need to have Tableau Reader version 2020.3.2 for report visualization.

Task 7. Dissemination of findings to VHA IE and other VHA Leadership
Brief VHA leadership, presenting a summary of findings to VHA IE and other VHA staff and answer questions about the methods used and how the Administration might use the findings to better plan and prepare for allocating resources in a national response to the COVID-19 public health emergency including the monitoring of adverse events and vaccine efficacy. The number of presentations will be determined by VHA IE. Not to exceed 25 presentations.

Deliverable: VHA Briefings - TBD

1.6 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

Title 38 of U.S. Code section 201. Veteran Health Information Systems and Technology Architecture, better known as VistA, 79VA10

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:
<u>Privacy Risk:</u> The Corporate Data Warehouse (CDW) contains sensitive personal information – including social security numbers, names, and protected health information. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

<u>Mitigation:</u> Veterans Health Administration (VHA), facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. Security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. Furthermore access to VAEC AWS cloud servers or CDW will require VHA credentials, using two factor authentications to login. Those security measures are inherited by this system.

Section 2. Uses of the Information

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

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

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

The Veterans Health Administration Ecosystem Innovation (VHA EI) will identify and protect those most vulnerable
beneficiaries from the COVID-19 coronavirus pandemic. Utilizing, a leading healthcare data science as a service firm, purpose-built machine learning platform called Visión. Visión provides a unique research-based platform combining advanced data science tools with seasoned healthcare domain expertise to realize actionable insights.

Utilizing the Visión platform VHA IE can fulfill the mission to identify COVID-19 vulnerable individuals with high precision, accuracy, and granularity. Further, the Vision platform integrates Social Determinants of Health, individual patient engagement levels (those with significant clinical risk with low medical system engagement), and patient-level propensity for obtaining vaccinations to identify other attributes of risk and barriers to health care resources. The combination of these features will allow for a workbench dashboard to be created that will identify Covid-19 vulnerable individuals as well as pathways for optimizing outreach and vaccination activities.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The project will leverage a data platform as a service, machine learning platform called Visión. The data created from the analysis will be used to create a workbench dashboard for clinician reference. The information dashboard output will be utilized to identify Covid-19 vulnerable individuals as well as pathways for optimizing outreach and vaccination activities. No data will be added to an individual medical record.

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

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

Add answer here:

Access to PII is determined by the currently assigned access level, contexts and roles. The application manager is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual, technical manual, and system design document.

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

Inputs for each production scoring utilizing the Vision Platform, for example, COVID-19 Clinical Condition, are ingested as part of the Data Management steps to prepare for production. Once ingested and validated, the Vision Platform runs the scoring for the clinical condition(s) and produces relevant Findings. Note, as other clinical conditions are included for scoring in the Vision Platform additional Data Requirements Detail ("Inputs" – standard data model), Data Dictionary COVID-19 (Inputs), and COVID-19 Workbench Pre-Aggregation Data Format ("Findings" outputs) will be generated and updated in substantially the same manner as the Covid-19 Clinical Condition example below.

COVID-19 Data Requirements Detail

COVID-19 Data Dictionary

After completion of each scoring production, weekly or monthly as agreed with the VA pursuant to contracted terms, Findings results will be published to VA (visual workbench and analytical reports as agreed pursuant to contracted terms), see COVID-19 Workbench Pre-Aggregation (outputs) below.

COVID-19 Workbench Pre-Aggregation Data

It is intended that upon publishing of the production scoring Findings to the VA that the underlying production data utilized Inputs will be wiped. The Findings in the form of visual workbench and analytical reporting will be retained. Each production run will include (i) data ingestion of Inputs from VA data sources, (ii) validation of data to standard data model, (iii) production run with output of Findings, with the final step (iv) being destruction of the underlying production input data, while retaining the published findings.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

This is clinical condition data viewed to be included in longitudinal analysis utilizing the Vision Platform. Published finding results will be retained pursuant to contracted terms between Cogitativo and the VHA. Patient Data is generated from the corporate data warehouse (CDW), which has a 75-year retention period upon no longer being seen in VA.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Chapter Six Health Care Records, Item No. III-6-1 (January 2019).

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

The authorized IT resources will handle all destruction and accumulate certifications for review and verification by CISO and or Manager ITSEC for attestation to Cogitativo Management and Client or Partner Management as applicable.

(System and destruction method)

All systems residing within the AWS environment have the capabilities to delete data after use. Once data is processed and no longer required, data destruction methods will be applied as required. Amazon Web Services (AWS) Redshift, Amazon Elastic Compute Cloud (Amazon EC2) and AWS Simple Cloud Storage (S3) bucket instances can be deleted after the analysis is completed. MySQL databases can be destroyed, and no data will be retained. Data stored in shared workspaces and MS Teams channels will be manually deleted. All backups will be purged from the AWS EC2 instances. Secure File Transfer Protocol (SFTP) accounts and directories will be digitally shredded.

Cogitativo Authorized Data Destruction

Cogitativo Data Classification and Handling Policy

Cogitativo Data Retention Policy

Cogitativo Data Retention Schedule

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Cogitativo will not use any PII for testing training or research. All work will be done by minimum necessary designated Cogitativo employees within the VA systems.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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 the information contained in the Data science machine learning platform, will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
OIT/ Corporate Data Warehouse (CDW)	Analysis of CDW data, to identify Covid-19 vulnerable individuals as well as pathways for optimizing outreach and vaccination activities.	Claim ID, Original claim id (for adjusted or rebilled/corrected claims), Member ID, Subscriber ID, Line of business (such as Medicare Advantage, ACA, Commercial, ASO, etc.), with ID and description, Service from and to dates, Servicing provider ID and NPI, Billing provider ID and NPI, Admitting diagnosis and version (ICD 9 v ICD 10), Primary diagnosis and version (ICD 9 v ICD 10), All other diagnosis codes (2-25) (facility claims), All procedure codes and ICD-10-PC (1-25) (facility claims), DRG code, Bill type (4-digit code), Claim status (accepted, pending, adjusted, etc.), Claim ID, Claim line number, Claim line service from and to dates,	Secure SSL

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Servicing provider ID and NPI, Billing provider ID and NPI, Place of service, Diagnosis codes (full set) and version (ICD 9 v ICD 10), Procedure codes (full set), Modifiers (1-4, or more, if available), Type of service code (professional claims), Revenue codes (facility claims), Claim line status (paid, pending, adjusted, denied), Member ID, Subscriber ID, Unique individual identifier, Member physical address, Member zipcode, Member preferred language, Member date of birth, Member gender, Member date of death (if applicable), Effective dates, Termination dates (eligibility history), Family relationship to subscriber ID, PCP Provider ID, Provider ID, Provider NPI	

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: The sharing of data is necessary for patients to be prioritized and receive a vaccine at a VHA facility. Privacy risk are limited by the fact that the final output on the workbench dashboard will be stripped of PHI. However, there is a risk that original data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy. The privacy risk would include the potential exposure of patient PHI, including any number of the 42 variables used in the machine learning process. The privacy exposure, in the hand of bad actors could allow for patient identity and diagnoses\comorbidities to be unwillingly disclosed. Such information could possibly be used against the patient or lead to fraud.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

If the VA suspects information has been significantly compromised, patients should be notified in writing. The notification will describe the specific data involved, the facts and circumstances surrounding the incident, the protective actions VA is taking

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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 question is 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.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP is giving out when the Veteran enrolls or when updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1) The VHA System of Record Notice (VHA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf

2) The VHA System of Record Notice (VHA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf

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

The Veterans' Health Administration (VHA) facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA

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

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

VHA permits individuals to agree to the collection of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by (VHACO)Veterans Health Administration Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

6.4 <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.

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

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

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

Follow the format below:
Privacy Risk: There is a risk that an individual may not understand why their information is being collected or maintained about them.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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.

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Right to Request Amendment of Health Information.

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

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

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

Information can also be obtained by contacting the facility ROI office.

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

<u>*Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.*</u>

Veterans and individuals should use the formal redress procedures addressed above.

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

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently affect the care the Veterans receive

Mitigation: As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records.

The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health l records and other records containing personal information. The Veterans' Health Administration (VHA) established My HealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy and Release of Information Directive 1605.01 establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

VA employees must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local area managers. Access is requested per policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once inside the system, individuals are authorized to access information on a need to know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

Access to computer rooms at facilities and regional data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Information stored in the Data science platform may be accessed by authorized VA employees. Access to file information is controlled using 2 factor authentications to the AWS servers and the employees are limited to only that information in the system which is needed in the performance of their official duties. We do not anticipate the need to download data from the data science platform system to be stored on government furnished equipment such as laptops or external hard drives.

Once authenticated into the system, authorized individuals are allowed to access information on a need to know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

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 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.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).
Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA (HIPAA) Health Insurance Portability and Accountability training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include in the

contract clarification of the mandatory nature of the training and the potential penalties for violating patient privacy.

Contractors must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees. All contractors who access the VA network will be required to sign a Confidentiality of Sensitive Information Non-Disclosure agreement. The contractor and any subcontractor(s) shall presume that the VA computer systems and storage media that the contractor or subcontractor access have sensitive information and applications, the modification or disclosure of which could cause significant harm or embarrassment to VA beneficiaries and employees and to VA's ability to perform its mission.

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

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

All VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training, including the VA Rules of Behavior (RoB) training. In addition, all employees who have access to Protected health information or access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused raining. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

ATO is in process and has not been completed for the Data science platform. The Initial Operating Capability date is April 15th, 2021. The system classified as moderate risk level per the categorization review.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Andrea J. Wilson 104706

Digitally signed by Andrea J. Wilson 104706
Date: 2021.03.22 15:53:48 -04'00'

PO, Andrea Wilson

Roland B Parten 596219

Digitally signed by Roland B Parten 596219
Date: 2021.03.22 12:28:02 -05'00'

Information Systems Security Officer, Roland Parten

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
Date: 2021.03.22 11:51:37 -05'00'

System Owner, Angela Gant-Curtis

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).

The Information Bulletin (IB) 10-163, Notice of Privacy Practices can be found at the following website: https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf