Privacy Impact Assessment for the VA IT System called:

Microsoft Power Platform

Veterans' Health/Corporate/Benefits Administration

Date PIA submitted for review:

9/12/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	gina.siefert@va.gov	202-632-8430
Information System Security Officer (ISSO)	Albert P. Comple	albert.comple@va.gov	318-466-2080
Information System Owner	Russell Holt	Russell.holt2@va.gov	970-9036991

Abstract

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

The Department of Veterans Affairs (VA) has made a significant investment in Microsoft technologies that includes the Microsoft Power Platform (MPP) which provides licenses for applications such as Microsoft Power BI, Power Apps, Power Apps Portals, Power Automate, Power Virtual Agent, and Dynamics 365. The Microsoft Power platform is a low-code, no-code app dev platform that is a multi-tenant application development platform that enables the rapid building, deployment and management of cloud-based applications using integrated graphical composition tools, metadata models, and software lifecycle management capabilities. Low-code, no-code app dev platforms encourage "citizen development." "Citizen development" enables organizations to transform their business exponentially faster because more users can create professional applications across the organization with rapidly built low-code apps that modernize processes and solve tough challenges.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.
The implementation of the Microsoft Power Platform (MPP) is managed, owned, and operated by Microsoft and their Center of Excellence Team.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
Microsoft PowerApps is a suite of apps, services, connectors and data platform that provides a rapid application development environment to build custom apps for business needs. Using PowerApps, customers can quickly build custom business apps that connect to business data stored either in the underlying data platform (Common Data Service) or in various online and on-premises data sources (SharePoint, Excel, Office 365, Dynamics 365, SQL Server, and so on). PowerApps includes the Portal, Authoring Service, and Robotic Process Automation. Microsoft Power Automate Power Automate is a service that helps organizations create automated workflows between applications and services to synchronize files, get notifications and collect data. The service provides a low code platform for workflow and process automation. Automated flows, button flows, scheduled flows, business flows and User Interface flows are supported by the service. Power BI Power BI is a suite of a collection of software services, apps, and connectors that work together to turn unrelated sources of data into sets of coherent, visually immersive, and interactive insights. The customer's data sources can include Excel spreadsheets or a combination of cloud-based and on-premises hybrid data warehouses. This business analytics tools assists the customer with data analysis

and insight sharing, business monitoring, and the ability to quickly find answers using rich visual dashboards available on every device. Dynamics 365 is Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) software package developed by Microsoft. With Dynamics 365, Microsoft is providing Dynamics functionality in the cloud through a SaaS model. The boxed Dynamics product and the SaaS product share the same codebase. The Dynamics 365 SaaS model allows users to coordinate workflow and develop metrics for business operations within an organization. The Dynamics 365 information system includes the following core services. Power Virtual Agent Version Date: May 1, 2021 Page 3 of 40 Power Virtual Agents (PVA) provides an integrated environment that can be created with a guided, no code graphical interface. The PVA service is offered in accordance with National Institute of Standards and Technology (NIST). Power Virtual Agents US Government plans include several features that allow users to connect to, and integrate with, other Microsoft enterprise service offerings such as Power Apps and Power Automate US Government. For purposes of FedRAMP ATO inheritance, Power Virtual Agents US Government plans use Azure (including Azure for Government) ATOs for infrastructure and platform services, respectively.

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

The implementation of the Microsoft Power Platform (MPP) is managed, owned, and operated by VA, Microsoft and their Center of Excellence Team

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The number of users whose information exists within the Microsoft Azure Government (MAG) environment not likely calculable given the scope, scale, and footprint of the environment across the entire VA enterprise

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

PII is collected for the purposes of authentication and authorization services by Azure Active Directory. Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. PII can be collected numerous ways throughout the Microsoft Azure Government environment: through connections to other system listed in the above, user input, by report aggregation, electronic transmission, or created by the system.

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

The Power Platform integrates to numerous databases and information repositories, both within the Azure for Government, VA enclaves and 3rd party SaaS applications. All connections for each use case are annotated on their respective Privacy Threshold Analysis (PTA) documents.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The Microsoft Power Platform describes a subset of low-code and no-code applications running in the Microsoft Azure for Government (MAG) environment, which is already FedRAMP authorized at a High Categorization

3. Legal Authority and SORN

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

Legal authorities to operate are identified in the High FedRAMP authorization as well as 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E. The completion of a PIA will not result in any technology changes. The existing SORN (SOR # 97VA10, Federal Register Citation # 85 FR 84119) covers cloud usage for the MAG environment

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The system is not in the process of being modified and the existing SORN (SOR # 97VA10, Federal Register Citation # 85 FR 84119) covers cloud usage for the MAG environment.

D. System Changes

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

N/A

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

N/A

Section 1. Characterization of the Information

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

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

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

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

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

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

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

PHI & patient demographics – Name, SSN, DOB, DOD, Age, Gender, Race, Veteran, Employee, Medical history including vaccination information, clinical risk factors, complications, reactions, treatments, dosage, and diagnosis. Phone number, Email, CAT-SS ID#, Address, Patient SID, Staff SID, Medication Information, Date of Admission (DOA) Patient Location (LOC), Ethnicity, Service Connection, Income, Prescription History, Order History, Consultation History, Immunization

History, Clinical Documentation Classification, Case identification, Patient ICN, Participation data (attendance, discharge reason), city, state, zip code, country, Branch of Military, Home Address, IP Address, Relationship to Veteran, Service Computation Date, Staff Seniority, Staff Position Numbers, Position Number, Suicide and Risk, Behavioral Health, Services received, Wellness & Recovery Information - Tools and Techniques, Plans for getting well safety, outcome, actions taken, outcome of the call, assessment, strategy used, VA Address, Mental Health Diagnosis, Disruptive Behavior Classification, Disruptive Behavior Description, Behavioral Protocols, Clinical Interventions, Suicidal Assessment Safety Events and Complaint Reports Safety Event and Complaint Investigation Files Physician first/last name, prescription drug name, Clinician Information: Name, login information, actions taken, outcome of the call, calendar, timestamps, assessment, strategy used, VHA Pharmacist name, EIN, scope of practice, credentials / training, and pharmacy location Employee name, email, contact number, duty station, department name(s) and assignments, occupational series, and date of bill, Email Address, , Phone Number, VA Email Address, Current Job Title, SSN, Name, Home Health Orders, Physician ID number, VSIN, Project name, Assessment score, VIPR number.

PII Mapping of Components (Servers/Database)

Microsoft Power Platform consists of 109 key components(databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Microsoft Power Platform and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection / Storage of PII	Safeguards
PBM_MUE workgroup	Yes	Yes	PHI & patient demographics – Name, SSN, DOB, DOD, Age, Gender, Race, Veteran, Employee, Medical history including vaccination information, clinical risk factors, complications, reactions, treatments, dosage, and diagnosis. Phone number, Email, CAT-SS ID#, Address, Patient SID, Staff SID, Medication Information, Date of Admission (DOA) Patient Location (LOC), Ethnicity, Service Connection, Income,	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

			Prescription History, Order History Consultation History, Immunization History, Clinical Documentation Classification, Case identification, Patient ICN, Participation data (attendance, discharge reason), city, state, zip code, country, Branch of Military, Home Address, IP Address, Relationship to Veteran, Service Computation Date, Staff Seniority, Staff Position Numbers, Position Number, Suicide and Risk, Behavioral Health, Services received, Wellness & Recovery Information - Tools and Techniques, Plans for getting well safety, outcome, actions taken, outcome of the call, assessment, strategy used, VA Address, Mental Health Diagnosis, Disruptive Behavior Classification, Disruptive Behavior Description, Behavioral Protocols, Clinical Interventions, Suicidal Assessment Safety Events and Complaint Reports Safety Event and Complaint Investigation Files Physician first/last name, prescription drug name, Clinician Information: Name, login information, actions taken, outcome of the call, calendar, timestamps, assessment, strategy used, VHA Pharmacist name, EIN, scope of practice, credentials / training, and pharmacy location Employee name, email, contact number, duty station, department name(s) and assignments, occupational series, and date of bill, Email Address, , Phone Number, VA Email Address, Current Job Title, SSN, Name, Home Health Orders,		

			Physician ID number, VSIN, Project name, Assessment score, VIPR number.		
D02_VISNXX DEV	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
VAWW.XX.VA.gov	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
crm9.dynamics.c	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
App Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Application Gateway	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Archive Storage	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access
Automation	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical

					isolation between each account, and logging of access.
Azure Active Directory	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Active Directory B2C	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Active Directory Domain Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Advanced Threat Protection	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Advisor	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Analysis Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure API for FHIR	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between

					each account, and logging of access.
Azure Bot Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Cache for Redis	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Cosmos DB	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Data Box Edge	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Data Box Pod & Disk Service	Yes	Yes		Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Data Explorer	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Data Lake Storage	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

Azure Data Movement	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Database for Maria DB	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Database for MySQL	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Database for PostgreSQL	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Database Migration Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Databricks	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure DDoS Protection	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Dedicated HSM	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in

					Time (JIT), logical isolation between each account, and logging of access.
Azure DevTest Labs	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure DNS	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Firewall	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Front Door Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Functions	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Information Protection	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure IoT Central	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between

					each account, and logging of access.
Azure IoT Hub	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Kubernetes Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Lab Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Machine Learning Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of acce
Azure Maps	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Migrate	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Monitor	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

Azure Monitor – Application Insights	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Monitor – Log Analytics	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure NetApp Files	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Portal	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Search	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Service Manager	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure SignalR Service	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure SQL Database	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in

					Time (JIT), logical isolation between each account, and logging of access.
Azure Stream Analytics	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Time Series Insights	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Azure Watson	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Backup	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Batch	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Cloud Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Cloud Shell	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between

					each account, and logging of access.
Cognitive Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Container Instances	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Content Delivery Network	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Content Moderator	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Cost Management	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Data Catalog	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Data Factory	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

Dynamics 365	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Event Hubs	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
ExpressRoute	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Face	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
HDInsight	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Import/Export	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Intune	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Key Vault	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in

					Time (JIT), logical isolation between each account, and logging of access.
Language Understanding	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Logic Apps	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Logic Apps – BAPI Connectors	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Machine Learning Studio	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Media Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Microsoft Cloud App Security	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Microsoft Flow	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between

					each account, and logging of access.
Microsoft Graph	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Microsoft PowerApps	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Microsoft Stream	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Mobile Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Multi-Factor Authentication	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Network Watcher	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Notification Hubs	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

Power BI	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Power BI Embedded	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
QnA Maker	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Scheduler	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Security Center	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Service Bus	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Site Recovery	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Sonar DaaS	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just i

Speech Services	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Storage	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
StorSimple	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Text Analytics	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Traffic Manager	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Translator Text	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Video Indexer	Yes	Yes	Same as above	Service functionality	Encryption of dat
Virtual Machines	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.

Virtual Machines Scale Sets	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Virtual Network	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
VPN Gateway	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Web Apps	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access.
Windows Defender ATP	Yes	Yes	Same as above	Service functionality	Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of 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?

Azure is aware of customers who provide PII through at a minimum Azure Active Directory; Azure treats all customer data uploaded to Azure Storage with the utmost sensitivity and only accesses that data as part of a support incident, and except through a support incident, Microsoft has no insight into what information customers upload to Azure Storage.

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.

For management of the service, Azure collects PII to provide authentication and access management services via at a minimum Azure Active Directory. Microsoft employee and contingent staff PII is also present to manage the system. Customers may populate the system with their users' PII.

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

No third-party sources are providing PII into the system.

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?

PII is collected for the purposes of authentication and authorization services by Azure Active Directory. Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current.

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

PII can be collected numerous ways throughout the Microsoft Azure Government environment: through connections to other system listed in the table above, user input, by report aggregation, electronic transmission, or created by the system.

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.

Where the PII is collected for the purposes of authentication and authorization, accuracy validation services are provided by at a minimum Azure Active Directory. Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. For amendment of incorrect data via the Azure Portal, tenant admins can correct as necessary. Microsoft also has a process via the Privacy Response Center to redress user submissions for correction or amendment of inaccurate PII. Please reference the Azure Online Services Terms for additional information

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

As of August 2018, under Appendix 1, Microsoft notes that personal data (PII) will be subject to the below processing activity:
"Customer Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf."

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

Legal authorities to operate are identified in the MAG High FedRAMP authorization as well as 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E SORN (SOR # 97VA10, Federal Register Citation # 85 FR 84119

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

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

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

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

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: VA employees utilize PII information in the Microsoft Azure Government environment, including connections to the Corporate Data Warehouse (CDW). Risks include misuse of PII and inaccuracy of data.

Mitigation: Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure. The Azure Privacy Officer is responsible for establishing policies and procedures to safeguard privacy across Azure services. All staff in an engineering role are required to take the annual training on standards of business conduct, which includes security and privacy. Contractors operate under NDAs, contractors with access to customer data and PII must sign additional contract addendums that ensure they understand and agree to Azure's privacy and data handling policies. Azure does not share PII data with other federal customers.

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.

Name: The patients name will be used for identification purposes.
Social Security Number: Will be used for identification purposes.
Phone Number: will be used to contact individual.
Date of Birth: Will be used for identification purposes or age and clinical relevance.
Current Medications: Will be used for clinical relevance.
Previous Medical Records: Will be used for clinical relevance.
Race/Ethnicity: Will be used for clinical relevance and identification.

Gender: Will be used for clinical relevance and gender identification
Date of Death: Will be used for clinical relevance.
Health Insurance Beneficiary Account Numbers: will be used to communicate and bill the third-party healthcare plans.
Email address: will be used to contact the individual.
Address: will be used for mailing purpose and identification
Position Number: will be used for identification.
Date of Admission: will be used for medical relevance.
SID (Special ID): will be used for identification.
Physician ID number: will be used for identification.
VSIN: will be used for VSIN identification.
Project Name: will be used for identification.
Assessment Score: will be used for assessment.
VIPR: will be used for tracking.

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.

Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. For amendment of incorrect data via the Azure Portal, tenant admins can correct as necessary. Microsoft also has a process via the Privacy Response Center to redress user submissions for correction or amendment of inaccurate PII. Please reference the Azure Online Services Terms for additional information

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.

As of August 2018, under Appendix 1, Microsoft notes that personal data (PII) will be subject to the below processing activity: “Customer Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1)

provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf."

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?

All Azure services implement internal controls as defined via the Microsoft Privacy Standard.

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

The Microsoft Privacy Standard is a corporate standard that identifies global privacy requirements across all Microsoft services. In order to protect SSNs-PII/PHI SFTP works over an SSH data stream to establish secure connection. Encryption algorithms securely move data to a server, keeping files unreadable during the process. To further prevent unauthorized files access, authentication is also enabled.

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

Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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.

2.4a How is access to the PII determined?

Access requests are assessed based on each user's role and responsibilities and whether they have a legitimate business need.

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

Access requests are assessed based on each user's role and responsibilities and whether they have a legitimate business need.

2.4c Does access require manager approval?

Access requests from within the team who manages the service are reviewed by that team's management.

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

Access requests from within the team who manages the service are reviewed by that team's management, requests from outside of the team are reviewed by that team's management and are available for auditing by the Azure Privacy Officer.

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

All Azure services implement internal controls as defined via the Microsoft Privacy Standard. The Microsoft Privacy Standard is a corporate standard that identifies global privacy requirements across all Microsoft services.

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*

DOD, medical history including vaccination information, clinical risk factors, complications, reactions, treatments, dosage and diagnosis; prescribing drug name and reason for use, branch of military, age, login information, action taken, training, pharmacy location, position number, security clearance type, employee ID, duty station, reporting to, name, veteran. Onboarding, PIV and background investigations, Employee relations, Performance management, Compensation and pay, GrpupID, User ID, Title, Project cost, Site URL, Domain name and ID, Cause of death, inpatient SID, Entity, ISO, ISSO, Product Owner, physician ID number, VIPR Number, assessment score, VSIN.

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.*

Azure's data handling policies dictate that customer data and PII tied to a customer must be retained as long as the subscription is active plus 90 days. At the end of the 90-day grace period customer data must be deleted within the subsequent 90 days.

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

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

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

Yes, the following data retention periods have been set and determined using approved VA and NARA guidance. Please reference the attached links below. Azure's data handling policies dictate that customer data and PII tied to a customer must be retained as long as the subscription is active plus 90 days. At the end of the 90-day grace period customer data must be deleted within the subsequent 90 days.

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

https://www.archives.gov/about/records-schedule

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

Data retention timelines are set and determined based on the different data types which are being handled and utilized within the application. The timeframe and duration applicable to each of the defined data categories is outlined accordingly for meeting the requirement of data retention and data disposal in a timely manner. The retention period and timeline set for each of the referenced

data types has been assessed accordingly through means of cybersecurity best practices. While also ensuring to adhere to all NARA approved retention periods and timelines set for different data categories. The retention period for each data category has been determined and has been set in accordance with all NARA approved timeframes outlined.

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.

Logical access to the data is removed and eventually overwritten when the sectors on the physical storage media are recycled. If a retired asset is evaluated and deemed to be accessible, it is destroyed onsite using an approved standard operating procedure that meets NIST SP-800-88 guidelines. These DBDs are physically and logically tracked to maintain chain of custody through final disposition.

Each Microsoft datacenter uses an on-site process to sanitize and dispose of failed and retired DBDs. During this process, Microsoft personnel ensure chain of custody is maintained throughout the disposal process. Purge and destroy sanitization are performed using tools and processes approved by the Security Group. Records are kept of the erasure and destruction of assets. Devices that fail to complete the clear are successfully degaussed (for magnetic media only), multi-pin punched (for chipped based boards such as SSDs) or destroyed.

A DBD is any storage device capable of storing customer or proprietary Microsoft data:

- Hard disk drives (HDD)
- Solid-state drives (SSD)
- USB drives
- IO Accelerator cards
- SD/Compact Flash cards
- HSM cards
- PCIe SSD cards
- NVDIMM (Non-Volatile Dual In-line Memory Module)

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the

risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII used for research, testing, or training, is required to be removed immediately after those functions have been completed, in accordance with the Acceptable Use Policy that the Business and Information Owner is required to sign. Testing environments can be re-baselined after test periods in order to accomplish this task as well.

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 the information contained in the Microsoft Power Platform Dataverse system 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: Azure's data handling policies dictate that customer data and PII tied to a customer must be retained as long as the subscription is active plus 90 days. At the end of the 90-day grace period customer data must be deleted within the subsequent 90 days.

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***
VHA VBA VACO	Information accessed, captured and shared in applications is for the improvement of services being delivered to	PHI & patient demographics – Name, SSN, DOB, DOD, Age, Gender, Race, Veteran, Employee, Medical history including vaccination information, clinical risk factors, complications, reactions, treatments, dosage, and diagnosis.	The connections to Microsoft Azure for Government is already approved by OIT and utilize

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	Veterans and creating efficiencies for employees delivering that service or supporting those services.	Phone number, Email, CAT-SS ID#, Address, Patient SID, Staff SID, Medication Information, Date of Admission (DOA) Patient Location (LOC), Ethnicity, Service Connection, Income, Prescription History, Order History Consultation History, Immunization History, Clinical Documentation Classification, Case identification, Patient ICN, Participation data (attendance, discharge reason), city, state, zip code, country, Branch of Military, Home Address, IP Address, Relationship to Veteran, Service Computation Date, Staff Seniority, Staff Position Numbers, Position Number, Suicide and Risk, Behavioral Health, Services received, Wellness & Recovery Information - Tools and Techniques, Plans for getting well safety, outcome, actions taken, outcome of the call, assessment, strategy used, VA Address, Mental Health Diagnosis, Disruptive Behavior Classification, Disruptive Behavior Description, Behavioral Protocols, Clinical	SFTP for data transfer.

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*
		Interventions, Suicidal Assessment Safety Events and Complaint Reports Safety Event and Complaint Investigation Files Physician first/last name, prescription drug name, Clinician Information: Name, login information, actions taken, outcome of the call, calendar, timestamps, assessment, strategy used, VHA Pharmacist name, EIN, scope of practice, credentials / training, and pharmacy location Employee name, email, contact number, duty station, department name(s) and assignments, occupational series, and date of bill, Email Address, , Phone Number, VA Email Address, Current Job Title, SSN, Name, Home Health Orders, Physician ID number, VSIN, Project name, Assessment score, VIPR number.	

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

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: There is a risk that information could be accessed by unauthorized individuals.

Mitigation: Microsoft Power Platform takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms: 1. The Application's loader API protected by a policy enforcement/policy decision point 2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services. 3. Data -at-rest encryption for any partition where PII will be contained 4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

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***
Dogs for Life, West Palm Beach, FL	VA staff will enter this information into the portal and have the option to assign veterans to a dog training organization (DTO) and cohort. DTO would view the veteran info and enter participation data (attendance, discharge reason from DTO). This information would be used to evaluate the PAWS program.	First, last name, Telephone number, Email address, Participation data (attendance, discharge reason)	Legal authorities to operate are identified in the High FedRAMP authorization as well as 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E. The completion of a PIA will not result in any technology changes. The existing SORN (SOR # 97VA10, Federal Register Citation # 85 FR 84119) covers cloud	SFTP All Azure services implement internal controls as defined via the Microsoft Privacy Standard. The Microsoft Privacy Standard is a corporate standard that identifies global privacy requirements across all Microsoft services. Security audit logging, controlled access via Azure JIT, and very

	Decisions such as: should the program continue? and should a larger scale be implemented?		usage for the MAG environment	limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.
PAWS for Purple Hearts, Anchorage, AK	Same as above	Same as above	Same as above	Same as above
PAWS for Purple Hearts, San Antonio, TX	Same as above	Same as above	Same as above	Same as above
Warrior Canine Connection, Ashville, NC	Same as above	Same as above	Same as above	Same as above
Warrior Canine Connection, Palo Alto, CA	Same as above	Same as above	Same as above	Same as above

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: There is a risk that information could be accessed by unauthorized individuals.

Mitigation: Microsoft Power Platform takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms: 1. The Application's loader API protected by a policy enforcement/policy decision point 2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services. 3. Data -at-rest encryption for any partition where PII will be contained 4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

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.

The VA publishes the SORN in the Federal Register under "Consolidated Data Information System-VA", SOR # 97VA10, Federal Register Citation # 85 FR 84119, located at https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf.

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

The VA publishes the SORN in the Federal Register under "Consolidated Data Information System-VA", SOR # 97VA10, Federal Register Citation # 85 FR 84119, located at https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf.

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.

The Privacy Impact Assessment is also completed for all use cases of Microsoft Power Platform applications that process or store PII/PHI.

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.

N/A. Microsoft Power Platform does not collect information directly from individuals, it only gathers pre-existing information located in various databases, reports, and repositories.

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.

N/A. Microsoft Power Platform does not collect information directly from individuals, it only gathers pre-existing information located in various databases, reports, and repositories.

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: Does not collect information directly from individuals, gathering pre-existing.

Mitigation: Microsoft Power Platform takes a defense-in-depth approach to protecting Employee PII data to include the following protection mechanisms: 1. The Application's loader API protected by a policy enforcement/policy decision point 2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services. 3. Data -at-rest encryption for any partition where PII will be contained 4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals requiring access to their information would be required to obtain that information from the original source.

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).

Individuals requiring access to their information would be required to obtain that information from the original source. As previously noted, Microsoft Power Platform does not collect information from or interact directly with individuals, the information is gathered from existing databases and repositories.

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.

As previously noted, Microsoft Power Platform does not collect information from or interact directly with individuals, the information is gathered from existing databases and repositories.

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.

Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. For amendment of incorrect data via the Azure Portal, tenant admins can correct as necessary. Microsoft also has a process via the Privacy Response Center to redress user submissions for correction or amendment of inaccurate PII. Please reference the Azure Online Services Terms for additional information. As of August 2018, under Appendix 1, Microsoft notes that personal data (PII) will be subject to the below processing activity: "Customer Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf."

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.

Not applicable as individuals do not have access to the information being presented.

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.

Not applicable as individuals do not have access to the information being presented.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Not applicable, does not collect information directly from individuals, gathering pre-existing.

Mitigation: Not applicable, does not collect information directly from individuals, gathering pre-existing.

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.

Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.

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?

Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.

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.

Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.

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.

Contractors are involved in the design, creation, and support of the Azure services. They all operate under NDAs, contractors with access to customer data and PII must sign additional contract addendums that ensure they understand and agree to Azure's privacy and data handling policies.

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 staff in an engineering role are required to take the annual training on standards of business conduct, which includes security, privacy, HIPPA, and VA Rules of Behavior.

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 Security Plan Status Date:* December 23, 2020
3. *The Authorization Status:* FedRAMP and VA authorized.
4. *The Authorization Date:* April 29, 2020
5. *The Authorization Termination Date:* April 29, 2023
6. *The Risk Review Completion Date:* April 29, 2020
7. *The FIPS 199 classification of the system:* HIGH

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

Yes, this is a Cloud SaaS. FedRAMP Package ID F1603087869.

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.*

In accordance with Microsoft ELA Contract GS-35F-0884P, the VA retains ownership of all information, including PII/PHI, throughout the entire Microsoft Azure Government environment and Microsoft Power Platform applications.

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.
Microsoft does not collect any ancillary data. All data used in Power Platform applications and within the MAG environment is owned by VA.

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.
Microsoft Azure Government and Microsoft Power Platform maintains compliance with all FedRAMP and VA security control requirements, to include all Privacy Overlay controls.

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).

Microsoft Power Automate utilizes RPA to create automated workflows via no-code and low-code interfaces and API's. https://powerautomate.microsoft.com/en-us/

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2023.09.27 16:54:47 -05'00'

Privacy Officer, Gina Siefert

ALBERT COMPLE Digitally signed by ALBERT COMPLE
Date: 2023.09.28 07:59:34 -06'00'

Information System Security Officer, Albert P. Comple

RUSSELL HOLT Digitally signed by RUSSELL HOLT
Date: 2023.09.28 08:04:41 -06'00'

Information System Owner, Russell Holt

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).

https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf.

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices