Privacy Impact Assessment for the VA IT System called:

Medical Care Collections Fund (MCCF) EDI TAS

Veterans Health Administration (VHA)

Office of Finance Revenue Operations, eBusiness Solutions

eMASS ID # 881

Date PIA submitted for review:

3/27/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rhonda Spry-Womack	Rhonda Spry-Womack@va.gov	615-613-2886
Information System Security Officer (ISSO)	Rito-Anthony Brisbane	Rito-Anthony.Brisbane@va.gov	512-460-5081
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

Medical Care Collections Fund (MCCF) EDI TAS is hosted on VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) high system. TAS supports the eBusiness product lines, which include eInsurance, ePharmacy, eBilling, and ePayments by providing infrastructure and services required for product teams to meet business requirements and objectives supporting third-party electronic revenue operations. TAS is responsible for the implementation of the technical foundation and framework to support modernized eBusiness.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

Medical Care Collections Fund (MCCF) EDI TAS. Office of Finance Revenue Operations, eBusiness Solutions

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

Medical Care Collections Fund (MCCF) EDI TAS is hosted on VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) high system. MCCF EDI TAS supports the eBusiness product lines, which include eInsurance, ePharmacy, eBilling, and ePayments by providing infrastructure and services required for product teams to meet business requirements and objectives supporting third-party electronic revenue operations.

MCCF EDI TAS is responsible for the implementation of the technical foundation and framework to support modernized eBusiness. The ownership/control of the IT system is the VA Enterprise Cloud (VAEC).

There are 800,000 expected number of clients stored in the system, a typical client is a Veteran or Veteran's family member receiving care from the VA. Information concerning outpatient pharmacy prescriptions and 3rd party insurance claims on same.

The purpose is to prepare a report (which displays no PII/PHI information) of insurance claims related to prescription activity in order to research and optimize claims recovery (i.e., revenue recovery for the VA) processes.

The information is used only by the ePharmacy Team for the research and process optimization activity noted above and is not shared with any other individual or team. The report, i.e., the ePharmacy No-Touch Report (NTR) is a module available only on the MCCF EDI TAS portal. The NTR is operated only from the TAS portal which is hosted on the Microsoft Azure Government (MAG) Cloud. The MCCF EDI TAS portal provides a secure link that launches the report. The MCCF EDI TAS system maintains security controls of the data used in the NTR. (Note: the NTR does not contain any PII/PHI.). Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.

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

VA Owned and VA Operated.

2. Information Collection and Sharing

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

There are 800,000 expected number of clients stored in the system, a typical client is a Veteran or Veteran's family member receiving care from the VA.

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

MCCF EDI TAS is responsible for the implementation of the technical foundation and framework to support modernized eBusiness. The purpose is to prepare a report (which displays no PII/PHI information) of insurance claims related to prescription activity in order to research and optimize claims recovery (i.e., revenue recovery for the VA) processes. The information is used only by the ePharmacy Team for the research and process optimization activity noted above and is not shared with any other individual or team. The report, i.e., the ePharmacy No-Touch Report (NTR) is a module available only on the MCCF EDI TAS portal. The NTR is operated only from the MCCF EDI TAS portal which is hosted on the Microsoft Azure Government (MAG) Cloud. MCCF EDI TAS portal provides a secure link that launches the report. The MCCF EDI TAS system maintains security controls of the data used in the NTR. (Note: the NTR does not contain any PII/PHI.). Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.

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

The information is used only by the ePharmacy Team for the research and process optimization activity noted above and is not shared with any other individual or team. The report, i.e., the ePharmacy No-Touch Report (NTR) is a module available only on the MCCF EDI TAS portal. The NTR is operated only from the TAS portal which is hosted on the Microsoft Azure Government (MAG) Cloud. The MCCF EDI TAS portal provides a secure link that launches the report. The TAS system maintains security controls of the data used in the NTR. (Note: the NTR does not contain any PII/PHI.). Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.

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

The system operates in the Microsoft Azure Government (MAG) Cloud.

3. Legal Authority and SORN

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

Public Law 99–272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986. MCCF EDI TAS processes information which is stored in VistA. The legal authority to operate the system is Title 38, United States Code, and Section 7301(a). The System of Records Notice is 79VA10, 'Veterans Health Information Systems and Technology Architecture (VistA) Records- VA.

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 SORN is associated with will not require a revision, amendment or approval.

4. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business processes.

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

Completion of this PIA will not potentially result in technology changes.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
□ Date of Birth
□ Mother's Maiden Name
□ Personal Mailing Address
□ Personal Phone Number(s)
□ Personal Fax Number
□ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Information
□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers[1]
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
☒ Medications
□ Medical Records
□ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
□ Gender
□ Integrated Control Number (ICN)
□ Military History/Service Connection
□ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Patient ID used for identification of patient, Prescriber ID use for identification of who prescribed.

PII Mapping of Components (Servers/Database)

MCCF EDI TAS consists of 1 key component (databases.). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MCCF EDI TAS and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
MCCF-PROD-INT-EAST SQL01	Yes	Yes	SSN, Patient Name, Patient ID, Drug Name	Data analysis and process optimization	PIA, encryption both at rest and in transit, VPN, and database assess is limited to MCCF EDI TAS CM staff

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?

The information is collected directly by VistA and accessed by the MCCF EDI TAS system through VistA data services. Please reference VistA documentation for details of the VistA files, sub-files and fields accessed by this system.

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.

MCCF EDI TAS system through VistA data services provide only for the information collected directly by VistA. Please reference VistA documentation for details of the VistA files, sub-files and fields accessed by this system

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

MCCF EDI TAS does not create information. The information is collected directly by VistA and accessed by the MCCF EDI TAS system through VistA data services. Please reference VistA documentation for details of the VistA files, sub-files and fields accessed by this system. MCCF EDI TAS will utilize tableau to display reports using data already accessed from VistA.

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?

The information is from VistA and accessed by the MCCF EDI TAS system through VistA data services. The data brought over to MCCF EDI TAS system side is checked daily by business users i.e., ePharmacy. The data is accessed via a data connector.

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

MCCF EDI TAS does not collect informatiion on a form. Information is provided from VistA data services then the data is brought over to MCCF EDI TAS 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.

MCCF EDI TAS does not check the accuracy from of information transmitted to it from VistA. The financial system is primarily concerned about the integrity of the data (during MCCF EDI TAS processing) not accuracy. The accuracy of the data is maintained by the data source which is VistA

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

MCCF EDI TAS does not check for accuracy. The accuracy of the data is maintained by the data source which is VistA

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*

In order to safeguard the retrieved SPI, we will take measures to ensure no data corruption or loss occurs, to include referential integrity (to ensure database consistency), encryption of data at rest and in transit and data checks (ex., checksums). The SORN (79VA10) Veterans Health Information Systems and Technology Architecture (VistA) Records-VA can be found at the following link: 2020-28340.pdf (govinfo.gov)

Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.

Public Law 99–272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986. MCCF EDI TAS processes information which is stored in VistA. The legal authority to operate the system is Title 38, United States Code, and Section 7301(a). The System of Records Notice is 114V.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: All sensitive information that is used by the system comes from VistA. The privacy risk to the sensitive information from VistA is moderate. There is a Moderate Loss of data integrity that could result in delay of claim processing, improper payment of claims or failure of VA recovery of funds from the 3rd party insurers. Incorrect data could result in improper billing for the wrong patient or billing for wrong care delivered, HIPPA fines, insurance fraud due to loss of ID, ID Theft, etc. Pharmacy deals with drug transactions and side effect check for multiple medicines. Inaccurate data or data loss could result in incorrect billing to the VA beneficiary (patient) with enforced mandatory recovery (e.g. from income tax refund checks). The result could be significant financial loss to the beneficiary. Data is Encrypted. Access is by those authorized for Privileges user accounts, need for access, least privilege access. System inherits cryptographic mechanisms to protect the confidentiality and integrity of remote access session. The system does not have publicly accessible content. The system retrieves the required information and packages it as part of the X12 transaction that is sent to Financial Services Center (FSC). These are normative procedures that need to occur in order to facilitate the revenue collection business processes at VA. Future releases may include the storage of PII/PHI data in order to facilitate reporting as specified by the eBusiness Solutions customer. This will be VistA data already in existence and not collected by MCCF EDI TAS. MCCF EDI TAS does not introduce any additional privacy risk with the use of the data from VistA.

Mitigation: MCCF EDI TAS enables electronic data exchange to and from VistA systems. MCCF EDI TAS components rely on the underlying enterprise infrastructure for file system protection as outlined in the Enterprise Infrastructure Support (EIS) SSPs. Application data is protected by user access permissions. Data confidentiality and integrity is also ensured via administrative, technical and physical controls.

Physical access to these servers is restricted to authorized personnel in a data center at a facility with 24- hour security. Network access to servers is managed through firewalls. Access via the network requires strong authentication for both the application and servers. Employing user logon access controls, strict VA and Office of Inspector General (OIG) policies with training, and a physically secure facility are all controls that aid in keeping the data confidential
VA 6500 implementation of this control states that database management systems used in VA will be encrypted using FIPS 140-2 (or its successor) validated encryption. Encryption of database management systems is currently implemented within MCCF EDI TAS.

Users will submit a completed access request application using a VA Form 9957. To ensure accountability, all user accounts are unique. Use of individual accounts is mandated.
Users are accountable for actions performed with their user ID and are held liable for actions determined to be intentionally malicious, grossly negligent, or illegal. All users must have a valid and authorized need to use the system.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	identification of patient	Not used
SSN	identification of patient	Not used
Patient ID	identification of patient	Not used
Drug Name	identification of what drug was prescribed	Not used
Prescriber ID	identification of who prescribed	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

MCCF EDI TAS includes a report writer module that will generate ad hoc and standardized reports to provide more detailed financial analysis. The reporting requirements have been developed by the business customer. The reporting package implemented is Tableau. It will be used to display reports that include the data described elsewhere in this document

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.

MCCF EDI TAS reporting package implemented is Tableau. It will be used to display reports that include the data described elsewhere in this document.

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?

Microsoft Azure Government (MAG) Cloud has built-in measures (i.e., Transparent Data Encryption) to protect data in transit and at rest.

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

None beyond the safeguards listed in the Section 1.1 table, i.e., IAM, data encryption, VPN and access limited to MCCF EDI TAS CM.

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

MCCF EDI TAS only allows remote access only with VA authentication and use a "time-out" function for remote access and mobile devices requiring user reauthentication after 15 minutes inactivity.

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. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

<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?

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information System

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

Yes, all employees and contractors with access to Veterans' information are required to complete VA Rules of Behavior and VA Privacy and Security training annually. Disciplinary actions, up to and including termination of employment, are possible for violations of the requirements specified in the training and their positions. These access rights are removed and reassigned for each transferred user, and these access permissions are re-approved annually.

2.4c Does access require manager approval?

Access is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the system.

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

Access is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the system.

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

All users of the system are responsible for assuring safeguards for the PII. The system manager is responsible for assigning users to the appropriate user roles to limit access and assuring PII safeguards as documented in the technical documentation and system design documentation.

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

No information is collected or retained. However, the information below will be used and may be reproduced that is stored on back-up systems which are used in the event of data loss occurs.

- Name: identification of patient
- Social Security Number (SSN): identification of patient
- Patient ID: identification of patient
- Drug Name: identification of what medication was prescribed
- Prescriber ID: identification of who prescribed

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.*

Retention period is seven (7) years for each electronic data transaction.

RCS 10-1 link for VHA: Records Control Schedule 10-1 (va.gov)• RCSVB- Part II
Revised for VBA: https://www.benefits.va.gov/WARMS/docs/regs/RCS_II.doc
National Archives and Record Administration: www.nara.gov

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

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

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

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

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

Retention schedule as approved by the VHA Record Control Schedule and the National Archives and Records Administration (NARA) GRS 1.1: Financial Management and Reporting Records General Records 1.1, Item 10: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. VHA RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdfGRS: https://www.archives.gov/records-mgmt/grs.html. The item Number 1260.1, Care in the Community, Disposition Authority N1-15-03-1, Item 2

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.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Disposition of Printed Data:

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

When feasible, the system uses fake patients for research, testing or training purposes. VHA Directive 1906 Data quality requirements for Healthcare Identity Management describes the requirements for using test patient information. Examples include "ZZZ Mickey Mouse" with an imitation/ Pseudo SSN "1234567890"

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

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by MCCF EDI TAS could 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 breach.

Mitigation: To mitigate the risk posed by information retention, the MCCF EDI TAS adheres to the VA RCS schedules for each category or data it maintains. When the retention date is reached for a record, the TAS system will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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***
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (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 may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of PIV two factor access to all VA systems access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and role-based access authorization are all measures that are utilized for the system.

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***
None				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: Not applicable, no external sharing

Mitigation: Not applicable, no external sharing

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 Notice of Privacy Practices is mailed to the Veteran at the time of enrollment. This mailing is handled by the HEC. If there are updates to the Notice of Privacy Practices, they are bulk mailed to all enrolled Veterans. Any non-Veteran requiring treatment will receive a Notice of Privacy Practices at the time of treatment. There are Notice of Privacy Practices in the facility in various locations and at all the Community Based Outpatient Clinics (CBOCs). The Notice of Privacy Practices can be found on the VA Privacy Service webpage (http://www.privacy.va.gov/Privacy_Resources.asp) by typing 'Notice of Privacy Practices' in the search box. The notice can also be found on the eHealth webpage (www.myhealth.va.gov) and at www.va.gov/vaforms by performing the same search for 'Notice of Privacy Practices'.

Also, on the Privacy Office SORN site are SORN 79VA10 Office of Privacy and Records Management

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

MCCF ED TAS does not collect information from the Veteran /non-Veteran. Sources collecting the information provide this notice.

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 Notice of Privacy Practices is mailed to the Veteran at the time of enrollment. This mailing is handled by the HEC. If there are updates to the Notice of Privacy Practices, they are bulk mailed to all enrolled Veterans. Any non-Veteran requiring treatment will receive a Notice of Privacy Practices at the time of treatment.

The Notice of Privacy Practices can be found on the VA Privacy Service webpage (http://www.privacy.va.gov/Privacy_Resources.asp) by typing 'Notice of Privacy Practices' in the search box. The notice can also be found on the eHealth webpage (www.myhealth.va.gov) and at www.va.gov/vaforms by performing the same search for 'Notice of Privacy Practices'.

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.

No information is directly collected from the Veteran by MCCF EDI TAS so there is no opportunity to decline to provide information.

A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems (such as VISTA) that collect the information from the Veteran MCCF EDI TAS. By declining to supply information to the source system, the Veteran would also be declining the information to the MCCF EDI TAS system and other downstream applications.

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.

Any right to consent to particular uses of the information would be handled by the source Systems that collect the information from the Veteran and feed MCCF EDI TAS with information

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

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

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

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

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

<u>Privacy Risk:</u> There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by MCCF EDI TAS.

<u>Mitigation:</u> Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1. MOU/ISA documents and business associate agreements along with the HIPAA Eligibility Transaction System (HETS) Trading Partner Agreement with CMS, provide a binding agreement and procedures to protect the data transferred.

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.***

See Appendix A for the notice of privacy practices provided at all VA medical centers, which includes the following: Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is Veteran's Service Record.

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)?

MCCF EDI TAS does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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?

MCCF EDI TAS does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review and obtain copies of their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Under the jurisdiction of VHA Directive 1605.01 Appendix D ‘Privacy and Release Information’, section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526.

The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately.

Reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

In addition to the written and published SORN as listed above, individuals seeking information regarding access to and contesting of records in this system may write or call the VHA Director of National Data Systems (19F4), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

There are no provisions for correcting inaccurate or erroneous information in MCCF EDI TAS. The information in MCCF EDI TAS is obtained via an interface with VISTA and FSC. MCCF EDI TAS derives its data from the source system VISTA. Individuals would not gain access to MCCF EDI TAS; instead, they would have to go through the source system's protocols to correct the data.

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: There is a risk that erroneous information is placed into MCCF EDI TAS via the feed from VistA.

Mitigation: The information in MCCF EDI TAS is obtained via interface with VISTA, and any information is obtained in VISTA. If there is erroneous or inaccurate information, it should be addressed in the VISTA system. Any validation performed would merely be the Veteran personally reviewing the existing information before they accept it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data through VISTA systems protocol.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Access by VA employees and VA contractors will be granted upon completion of the VA Privacy and Information Security Awareness training including HIPAA, VA National Rules of Behavior (ROB) or VA Contractor's ROB training; re-affirming their acceptance annually.

Specified access is granted based on the employee’s functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

Additionally, MCCF EDI TAS will leverage internal authentication and authorization mechanisms, but the expectation is that prior to national deployment, access services will be provided by the IAM program, including SSOi. The components that run on VistA servers will leverage VistA access management controls. Many of the controls for MCCF EDI TAS will be inherited either nationally or by the Enterprise Operations and Field Operations common controls from the service lines. These controls also apply to MCCF EDI TAS components running within the EO cloud within the Regional Data Centers.

Connections to and from VistA via REST Resources will all be bound by Hypertext Transfer Protocol Secure (HTTPS) connections. Access to PHI and PII is only allowed in production environments. VistA REST Resources can only be deployed to those environments after Authorization to Operate (ATO) compliant testing has been completed. No PHI or PII is allowed in development environments.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No other agencies have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Access is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

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 can be granted access if their VA manager, COR and system Information Security Officer (ISO) approves. They are required to follow the same procedures VA employees do for access. In accordance with the contract between the contractor and the government, all contractors with access are required to meet VA contractor security requirements including reaffirming annual completion of specific security training: VA Privacy and Information Security Awareness and Rules of Behavior and Privacy and HIPAA Training. For those granted elevated privileges, Information Security Role-Based Training for System Administrators (WBT) training is also required annually, and a quarterly review and re-approval of elevated privileges is required by the COR to maintain elevated privileges.

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.

Privacy and Security training is a requirement at VA, and all relevant VA-wide trainings are completed by all personnel annually. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the HIPAA, VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security Awareness training, which all personnel must complete via the VA’s Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training.

Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS.

In addition, the eBusiness Solutions Office manages the development, implementation and ongoing support of the Department of Veterans Affairs (VA) Electronic Data Interchange (EDI) applications within VistA by providing training to VA Medical Center (VAMC) and Consolidated Patient Account Center (CPAC) staff on the updated EDI software, including program support to staff and trading partners

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Denied
2. *The System Security Plan Status Date:* 10/18/2021
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 11/18/2021
5. *The Authorization Termination Date:* 11/17/2024
6. *The Risk Review Completion Date:* 11/9/2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

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)*

MCCF EDI TAS utilizes the VAEC Microsoft Azure Government (MAG) Cloud and is characterized as an IaaS.

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.*

MCCF EDI TAS utilizes the VAEC Microsoft Azure Government (MAG) Cloud and is characterized as an IaaS.

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.

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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).

<<ADD ANSWER HERE>>

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

RHONDA SPRY-WOMACK

Digitally signed by RHONDA SPRY-WOMACK
Date: 2024.05.07 12:45:07 -05'00'

Privacy Officer, Rhonda Spry-Womack

RITO-ANTHONY BRISBANE

Digitally signed by RITO-ANTHONY BRISBANE
Date: 2024.05.07 13:21:33 -05'00'

Information System Security Officer, Rito-Anthony Brisbane

TONY SINES

Digitally signed by TONY SINES
Date: 2024.05.07 13:43:01 -05'00'

Information System Owner, Tony Sines

APPENDIX A-6.1

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

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES

- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)

- 2013 *https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090*

https://www.oprm.va.gov/privacy/systems of record.aspx

Department of Veterans Affairs-Veterans Health Administration
NOTICE OF PRIVACY PRACTICES
Effective Date September 23, 2013
THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY.
The Department of Veterans Affairs' (VA) Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA is also required to abide by the terms of this Notice and its privacy policies.
How VHA May Use or Disclose Your Health Information without Your Authorization

(See below for more information about these categories)
□ Treatment (e.g., giving information to VHA and other doctors and nurses caring for you)
□ Payment (e.g., giving information to non-VHA facilities that *provide care or services*
□ *Health Care Operations (e.g., giving information to individuals conducting Quality of Care reviews)*
□ *Eligibility and Enrollment for VA Benefits (e.g., giving information to officials who decide benefits)*
□ *Abuse Reporting (e.g., giving information about suspected abuse of elders or children to government agencies)*
□ *Health or Safety Activities*
□ *Public Health Activities (e.g., giving information about certain diseases to government agencies)*
□ *Judicial or Administrative Proceedings (e.g., responding to court orders)*

□ Law Enforcement
□ Health Care Oversight (e.g., giving information to the Office of Inspector General or a Congressional Committee)
□ Cadaveric Organ, Eye, or Tissue Donation
□ Coroner or Funeral Activities
□ Services (e.g., giving information to contractors or business associates performing services for VHA)
□ National Security Matters
□ Workers' Compensation Cases (e.g., giving information to officials who decide payments for workplace injuries Payment (e.g., giving information to non-VHA facilities that provide care or
□ services)
□ Correctional Facilities
□ When Required by Law
□ Activities Related to Research (e.g., certain activities with only minimal or limited privacy or confidentiality risks)
□ Planning VA research projects (e.g., investigator accesses, but does not disclose or record, individual health information to determine feasibility of opening a study)
□ Military Activities (e.g., giving information to the Department of Defense (DoD)
□ Academic Affiliates (e.g., giving information to assist in training medical students)
□ State Prescription Drug
□ Monitoring Program (SPDMP) reporting and query
□ General Information Disclosures (e.g., giving out general information about you to your family and friends)
□ Verbal disclosures to others while you are present
□ Verbal Disclosures when you are not present (e.g., assisting Family Members or Designated Individuals Involved in your Care)

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose based on a signed, written authorization you provide us. Your signed written authorization is always required to disclose your psychotherapy notes if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed written authorization, we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Revocation of Authorization. If you provide us a written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization.

YOUR PRIVACY RIGHTS Right to Request Restriction.
You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, we are not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you no longer make the restriction request valid or you revoke it.

NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.
NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is http://www.archives.gov/veterans/military-service-records/medical-records.html.

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

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

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

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website, http://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089
Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you should take, if any.
Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

- □ The VHA health care facility’s Privacy Officer, where you are receiving care. Visit this Web site for VHA facilities and telephone numbers http://www1.va.gov/directory/guide/division_flsh.asp?dnum=1.

- □ VA via the Internet through “Contact the VA” at http://www.va.gov; by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10P2C1) at 810 Vermont Avenue NW, Washington, DC 20420.
- □ The U.S. Department of Health and Human Services, Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
- □ The Office of the Inspector General. http://www.va.gov/oig/contact/default.asp
- □ Complaints do not have to be in writing, though it is recommended.
- □ An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

Changes. We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes we will make available to you a copy of the revised Notice within 60 days of any change.
When We May Use or Disclose Your Health Information without Your Authorization Treatment.
We may use and disclose your health information for treatment or to provide health care services. Treatment may include:

- □ Emergency and routine health care or services, including but not limited to labs and x-rays; clinic visits; inpatient admissions

□ Contacting you to provide appointment reminders or information about treatment alternatives

- □ Prescriptions for medications, supplies, and equipment
- □ Coordination of care, including care from Non-VHA providers
- □ Coordination of care with DoD, including electronic information exchange

NOTE: If you are an active duty service member, Reservist or National Guard member, your health information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD’s access to your information in this database, even if you ask us to do so.
Examples:
1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran’s health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital that needs the information to treat this Veteran.
3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.
Payment. We may use and disclose your health information for payment purposes or to receive reimbursement for care provided, including: Determining eligibility for health care services

- □ Paying for non-VHA care and services, including but not limited to, CHAMPVA and fee basis
- □ Coordinating benefits with other insurance payers
- □ Finding or verifying coverage under a health insurance plan or policy
- □ Pre-certifying benefits
- □ Billing and collecting for health care services provided
- □ Providing personal information to consumer reporting agencies regarding delinquent debt owed to VHA
- □ Allowing you to pay for your health care out of pocket so that your insurance is not billed

Examples:
1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran’s health information to determine eligibility for health care services.
2) The VHA health care facility discloses a Veteran’s health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.

Health Care Operations. We may use or disclose your health information without your authorization to support the activities related to health care, including:

- □ Improving quality of care or services
- □ Conducting Veteran and beneficiary satisfaction surveys
- □ Reviewing competence or qualifications of health care professionals
- □ Providing information about treatment alternatives or other health-related benefits and services
- □ Conducting health care training programs
- □ Managing, budgeting and planning activities and reports
- □ Improving health care processes, reducing health care costs and assessing care costs and assessing organizational performance
- □ Developing, maintaining and supporting computer systems
- □ Legal services
- □ Conducting accreditation activities
- □ Certifying, licensing, or credentialing of health care professionals
- □ Conducting audits and compliance programs, including fraud, waste and abuse investigations

Examples:
1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality of care review process to determine if the care was provided in accordance with the established best clinical practices.
2) A VHA health care facility discloses a Veteran’s health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.

Eligibility and Enrollment for Federal Benefits. We may use or disclose your health information to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service or Social Security Administration, to determine your eligibility for Federal benefits.

Abuse Reporting. We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

Health and Safety Activities. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

Public Health Activities. We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. Public health activities may include:

- □ Controlling and preventing disease, injury, or disability
- □ Reporting vital events such as births and deaths
- □ Reporting communicable diseases such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- □ Tracking FDA- Regulated products
- □ Enabling product recalls, repairs or replacements
- □ Reporting adverse events and product defects or problems

Judicial or Administrative Proceedings. We may disclose your health information without your authorization for judicial or administrative proceedings, including:

- □ We receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure
- □ To defend VA in judicial and administrative proceedings

Law Enforcement. We may disclose your health information to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. These law enforcement purposes may include:

- □ Identifying or apprehending an individual who has admitted to participating in a violent crime
- □ Routine reporting to law enforcement agencies, such as gunshot wounds

Health Care Oversight. We may disclose your health information to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

Cadaveric Organ, Eye, or Tissue Donation. When you are an organ donor and death is imminent, we may use or disclose your relevant health information to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for the purpose of determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

Coroner or Funeral Services. Upon your death, we may disclose your health information to a funeral director for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

Services. We may provide your health information to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contract and business associate agreement must be in place securing your information.
National Security Matters. We may use and disclose your health information without your authorization to authorized Federal officials for the purpose of conducting national security and intelligence activities. These activities may include protective services for the President and others.

Workers' Compensation. We may use or disclose your health information without your authorization to comply with workers' compensation laws and other similar programs.

Correctional Facilities. We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; to protect the health and safety of you or others; or for the safety of the facility.

Required by Law. We may use or disclose your health information for other purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

Activities Related to Research. Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

- □ A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.
- □ The IRB approves a waiver of informed consent and a waiver of authorization to use or disclose health information for the research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- □ A Limited Data Set containing only *indirectly* identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

Military Activities. We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active Duty Service members and in some cases Reservist and National Guard members. An example of a military activity includes the disclosure of your health information to determine fitness for duty or deployment to your Base Commander.

Academic Affiliates. We may use or disclose your health information, without your authorization, to support our education and training program for students and residents to enhance the quality of care provided to you.

State Prescription Drug Monitoring Program (SPDMP). We may use or disclose your health information, without your authorization, to a SPDMP in an effort to promote the sharing of prescription information to ensure appropriate medical care.

General Information Disclosures. We may disclose general information about you to your family and friends. These disclosures will be made only as necessary and, on a need,-to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- □ Verification of identity
- □ Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- □ Your location in a VHA health care facility (e.g., building, floor, or room number)

Verbal Disclosures to Others While You Are Present. When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. For example, your doctor may talk to your spouse about your condition while at your bedside. Before we make such a disclosure, we will ask you if you object. We will not make the disclosure if you object.

Verbal Disclosures to Others When You Are Not Present. When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person's involvement with your health care or payment for your health care. Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

IMPORTANT NOTE: A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care only if we have your signed, written authorization or if the individual is your authorized surrogate (the individual who is authorized to make health care decisions on your behalf if you can no longer do so) and the practitioner determines that the information is needed for the individual to make an informed decision regarding your treatment.

When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information
Patient Directories. Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name. If you do object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.

When We Will Not Use or Disclose Your Health Information

Sale of Health Information. We will not sell your health information. Receipt of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA fees is not a sale of health information.

Genetic Information Nondiscrimination Act (GINA). We will not use genetic information to discriminate against you either through employment or to determine your eligibility for VA benefits.

Contact Information.
You may contact your VHA health care facility's Privacy Officer if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Informatics and Analytics (10P2C1), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038.

HELPFUL LINKS:

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

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

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

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

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