Privacy Impact Assessment for the VA IT System called:

Fee Basis Claims Archive (FBCA)

Veteran Health Administration (VHA)
Office of Community Care

Date PIA submitted for review:

29 June 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	michael.hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Ashton Botts or James Alden	Ashton Botts or James.Alden@va.gov	303-398-7155 or 781-687-4779
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?" and will be published online to accompany the PIA link.

Fee Basis Claims Archive (FBCA) is a SQL Server Reporting Services application used for reporting historical Fee Basis Claims System Data after FBCS is sunset at each VISN. FBCA will not be connected to any external or internal systems. It will allow users within VHA to connect using a web server to verify health claim information processed between 2010 through 2020.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

Fee Basis Claims Archive (FBCA) is a Veterans Health Information Systems and Technology Architecture (VistA)-integrated claims processing and management system. Business owner: Office of Community Care.

It will allow users within VHA to connect using a web server to verify health claim information processed between 2010 through 2020. FBCA is a SQL Server Reporting Services application used for reporting historical Fee Basis Claims System Data after FBCS is sunset at each VISN. Previous number of individuals that access the Fee Basis Claims System when processing claims were 6032. We expect up to 4000 initially on FBCS Archive but will gradually go down after 4 – 5 years to a few hundred VA employee users. Users are considered those individuals in VHA groups: Revenue,

Clinical Integration, Customer Service, Appeals, Informatics; and Payment Operations Management requiring access to perform their duties.
Fee Basis Claims Archive (FBCA) is a Veterans Health Information Systems and Technology Architecture (VistA)-integrated claims processing and management system. FBCA will not be connected to any external or internal systems. The On-Prim FBCS Archive is only operated at Cleveland, so there is no issue maintaining consistency between sites. There is approximately 2 million Veteran and their relatives in FBCA with the same information stored from Fee Basis Claims System. As stated earlier, the information stored was date that was used to verify health claim information processed between 2010 through 2020.

Legal Authorities to Operate:
38 U.S.Code. § 501 - VETERANS' BENEFITS Rules and regulations
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720G - Assistance and support services for caregivers
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, NC
38 U.S. Code § 1802-Children of Vietnam Veterans Born with Spina Bifida-Spina Bifida conditions
1803, Sec. 1803 - Children of Vietnam Veterans Born with Spina Bifida-Spina Bifida -Health care
1812, 38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects
1813, 38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects-Health Care
38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida
Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities.
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
Public Law 111–163 section 101. Caregivers and Veterans Omnibus Health Services Act of 2010- Sec. 101. Assistance and support services for caregivers.
5 U.S.C. § 301 - Departmental regulations
26 U.S. Code § 61 - Gross income defined (a) **(12)** Income from discharge of indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for discharged members of allied forces
38 U.S. Code § 111 - Payments or allowances for beneficiary travel
38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation
38 U.S. Code § 1705 - Management of health care: patient enrollment system
38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care
38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines
38 U.S. Code § 1717 - Home health services; invalid lifts and other devices
38 U.S.C. § 1721 – Power to make rules and regulations
38 U.S.C. § 1727 - Persons eligible under prior law
38 U.S.C. 1741-1743. Per Diem Grant- State Home
38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care
38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program
38 U.S. Code § 5701 - Confidential nature of claims
38 U.S. Code § 5724 - Provision of credit protection and other services

38 U.S. Code § 5727 – Definitions
38 U.S. Code § 7105 - Filing of notice of disagreement and appeal
38 U.S. Code § 7332 - Confidentiality of certain medical records
38 U.S.C. 8131-8137. Construction Grant- State Home
44 USC - PUBLIC PRINTING AND DOCUMENTS
Veterans Access, Choice, and Accountability Act of 2014
38 CFR 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).
TITLE 45 CFR-Public Welfare Subtitle A-Department of health and Human Services-Part 160-General Administrative Requirements
45 CFR Part 164 – Security and Privacy
4 CFR 103 – Standards for the Compromise of Claims
Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:
Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug. 21, 1996, (codified in scattered sections of Title 42 U.S.C.)(full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
Health Information Technology for Economic and Clinical Health (HITECH) Act**,** Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Action of 2009 ARRA, Pub. L. No. 111-5, 123 Stat. 226 (Feb.17, 2009), *codified* at 42 U.S.C. §§300jj *et seq*.; §§17901 *et seq*.

Completion of this PIA will not result in changes to the business process. The archive of this system has changed technology processes, but the completion of this PIA will not. No SOR will need to be amended or revision due to this system. This system does not use cloud technology.

As with any disclosure, if privacy related data is disclosed intentionally or unintentionally would cause very bad publicity to the Department of Veteran Affairs and would most likely the department would have multiple lawsuits and the dismissal of personnel that had caused the incident.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☒ Previous Medical Records
- ☒ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☒ Other Unique Identifying Information (list below)

Veteran service-connected status and conditions, zip code, gender, Medical Claim data and financial records.

PII Mapping of Components

Fee Basis Claim Archive (FBCA) consists of 0 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FBCA and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

As FBCA is an archive repository which maintains the data from Fee Basis Claim System (FBCS) a minor application to Veterans Health Information Systems and Technology Architecture (VistA) Fee.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

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

FBCA is data archive storage which was once maintained in the Fee Basis Claim System (FBCS). FBCA does not have any database, internal or external connections.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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

FBCA is a repository that maintains data, there will be no automated or VA employee data verifications for accuracy. FBCA will be accessible to retrieve data only.

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

38 U.S.Code. § 501 - VETERANS' BENEFITS Rules and regulations
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720G - Assistance and support services for caregivers
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, NC
38 U.S. Code § 1802-Children of Vietnam Veterans Born with Spina Bifida-Spina Bifida conditions
1803, Sec. 1803 - Children of Vietnam Veterans Born with Spina Bifida-Spina Bifida -Health care
1812, 38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects
1813, 38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects-Health Care
38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida
Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities.
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
Public Law 111–163 section 101. Caregivers and Veterans Omnibus Health Services Act of 2010- Sec. 101. Assistance and support services for caregivers.
5 U.S.C. § 301 - Departmental regulations
26 U.S. Code § 61 - Gross income defined (a) (12) Income from discharge of indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for discharged members of allied forces
38 U.S. Code § 111 - Payments or allowances for beneficiary travel
38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation
38 U.S. Code § 1705 - Management of health care: patient enrollment system
38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care
38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines
38 U.S. Code § 1717 - Home health services; invalid lifts and other devices
38 U.S.C. § 1721 – Power to make rules and regulations
38 U.S.C. § 1727 - Persons eligible under prior law
38 U.S.C. 1741-1743. Per Diem Grant- State Home
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, NC
38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program
38 U.S. Code § 5701 - Confidential nature of claims
38 U.S. Code § 5724 - Provision of credit protection and other services

38 U.S. Code § 5727 – Definitions
38 U.S. Code § 7105 - Filing of notice of disagreement and appeal
38 U.S. Code § 7332 - Confidentiality of certain medical records
38 U.S.C. 8131-8137. Construction Grant- State Home
44 USC - PUBLIC PRINTING AND DOCUMENTS
Veterans Access, Choice, and Accountability Act of 2014
38 CFR 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).
TITLE 45 CFR-Public Welfare Subtitle A-Department of health and Human Services-Part 160-General Administrative Requirements
45 CFR Part 164 – Security and Privacy
4 CFR 103 – Standards for the Compromise of Claims

The VistA operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C), Chapter 5, §501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a).

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

• Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug. 21, 1996, (codified in scattered sections of Title 42 U.S.C.)(full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

• Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Action of 2009 ARRA, Pub. L. No. 111-5, 123 Stat. 226 (Feb.17, 2009), *codified* at 42 U.S.C. §§300jj *et seq*.; §§17901 *et seq*.

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.

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: Data maintained in the FBCA collection is not accurate or complete.

Mitigation: All Personally Identifiable Information (PII) was validated at the time of collection in the FBCS system before migrated to the FBCA System.

Section 2. Uses of the Information

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

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

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

Note the data was collected in the live system for the following uses, in the FBCA system the use will be for claim look up or reporting purposes.

Data Element	Use
Name	To accurately identify the Veteran
Social Security Number	To accurately identify the Veteran
Date of Birth	To accurately identify the Veteran
Mailing Address	To complete correspondence addressed to the Veteran
Zip Code	To complete correspondence addressed to the Veteran
Health Insurance Beneficiary Numbers	To render fee basis claim decisions
Internet Protocol Address Numbers	To connect to interfacing systems (these IPs are not for individuals)
Previous Medical Records	To render fee basis claim decisions
- Medical Claim Forms	To render fee basis claim decisions against
- Electronic Medical Claim Submissions	To render fee basis claims decisions
Veteran Service-Connected Status/Conditions	To render fee basis claims decisions
Tax Identification Number	To render fee basis claims decisions
Race/ethnicity	To accurately identify the Veteran
Gender	To accurately identify the Veteran
Financial records.	To render fee basis claims decisions

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

FBCA will allow VA employees to connect using a web server to verify health claim information processed between 2010 through 2020. No changes to the records can be made as these are "read only" records.

2.3 How is the information in the system secured?

2.3a What measures are in place 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?

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

The security controls include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The FBCA team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected. There are no additional protections at this time besides VA continual training to provide protection to all PII/PHI data. Data is encrypted at rest and in transit. Access to the system is Two-Factor Authenticated (2FA) via the VA's Identity Access Management (IAM) system and further restricted by VA's Form 9959 approval and business owner approval. Application automatically *times out after 15 minutes of inactivity to protect on-screen displays.*

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Access is given to individuals as a need to know to perform their job to answer questions required concerning Veterans or Providers for those Veterans. Criteria and procedures/controls are maintained by VHA regarding access to Veteran information. A User Administrator controls access for all users of the FBCS Archive Application. Access is tracked, monitored and recorded, and access is removed if not used within 90 days. Each group (Appeals, Clinical Integration, Customer Service, Revenue, Informatics, and Payment Operations Management) as well as OIT are all responsible for assuring safeguards for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name, Social Security Number (SSN), Date of Birth (DOB), personal mailing address, health insurance beneficiary numbers account numbers, previous medical records, Veteran service-connected status and conditions, zip code, race, gender, Medical Claim data and financial records

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Records in FBCA will be retained per the Veteran Health Administration Record Control Schedule 10-1, 4000- Financial Management and Reporting Records, (b) Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

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

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

Yes, Veteran Health Administration Record Control Schedule 10-1, 4000- Financial Management and Reporting Records, (b) Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting.
RCS 10-1: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

At the end of the retention period, 6 years after final payment or cancellation, but longer retention is authorized if required for business use. The system will be decommissioned following the VHA Records Management policy, VHA Directive 6300 and Electronic Media sanitation: VA Handbook 6500, Information Security Program, Information System Hardware and Electronic Media Sanitization and Disposal, Policy: VA's electronic media sanitization procedures for electronic media are to be followed. These procedures ensure that electronic media are appropriately sanitized or destroyed; the action has been documented; and all VA sensitive information is protected to prevent subsequent disclosure when OI&T equipment containing VA sensitive information is surpluses, donated, or otherwise removed from VA control. Procedure: The facility will ensure that sanitization of VA sensitive information from equipment is accomplished before the equipment is released from custody for disposal. This sanitization

process must cause the removal of all VA sensitive information from information systems storage devices and render the information from these systems unreadable. The OI&T Chief/CIO will be responsible for identifying and training OI&T staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

The data maintained in this system will not be used in research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:
Privacy Risk: Data in the system is retained past the retention period, the availably of the data would present for litigation, or Freedom of Information Act requests.

Mitigation: This a data repository and will be monitored and purged 6 years after final payment or cancellation, but longer retention is authorized if required for business use per the VHA Record Control Schedule 10-1.

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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
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.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Data maintained in the system is accessible to pull reports and access previously processed claims, historical data, risk exposure if access is not monitored.

Mitigation: For FBCA on prem (Cleveland) it's continuous monitoring. Monthly Nessus scans, POAMs for said scans, lather rinse repeat. Same for all other scans. Annual, or as required. In addition, Access is controlled by each group having access to FBCS Archive. The groups are Revenue, Clinical Integration, Appeals, Customer Service, Informatics, and Payment Operations Maintenance. All groups have User Administrators assigned which approves users for their group, and VHA has a process in place for periodic review of all users. In addition, the application has a control that removes access for an individual if they have not logged in within 30 days, and a User Administrator has to again approve a new registration each time.

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 3.11 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	***List the purpose of information being shared /***	***List the specific PII/PHI data elements that are***	***List the legal authority, binding***	***List the method of transmission and the***

information is shared/received with	*received / transmitted with the specified program office or IT system*	*shared/received with the Program or IT system*	*agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*measures in place to secure data*
N/A				

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

In accordance with M-06-16, we 1. Ensure we encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing; 2. Our application allows remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; 3. Our application uses a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes inactivity.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Information is not shared with external organization.

Mitigation: Not Applicable.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

HIPAA requires providers to provide notices to patients of the use of patient data for the purposes of processing insurance payments at the point of service. VA provides a notice of privacy practices every 3 years mailed to Veterans. Beneficiaries are notified upon eligibility and through the CHAMPVA guide.

1. Systems of Record Notices outline the collection and use of information in each of these SORNS:
   (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
   (1) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
   (2) 24VA10V7/85FR62406, Patient Medical Records-VA (10-2-2020)
   (3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
   (4) 79VA10/85FR84114 Veteran Health Information Systems and Technology Architecture (VistA) Records-VA (12-23-2020)

2. This Privacy Impact Assessment (PIA) also serves as notice.
As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

3. For VHA related Privacy Notification online can be found at: http://www.va.gov/health/ after getting to the website select VA Privacy Practices link on the lower right side of the web page.

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

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

Yes, individuals have the right to decline disclosure during process, but this is a post-production historical archive, so no claim processing is affected in the archive. Any consenting would have been while their information was active, and at this time if permission is revoked, we would not be able to answer questions about past activities from either Veterans or Vendors.

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

Yes, individuals have the right to decline disclosure during process, but this is a post-production historical archive, so no claim processing is affected in the archive. Any consenting would have been while their information was active, and at this time if permission is revoked, we would not be able to answer questions about past activities from either Veterans or Vendors.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice from the originating source that their information is being collected, maintained, processed, or disseminated by individuals using the FBCS Archive.

Mitigation: HIPAA requires providers to provide notices to patients of the use of patient data for the purposes of processing insurance payments at the point of service. VA provides a notice of privacy practices every 3 years mailed to Veterans. Beneficiaries are notified upon eligibility and through the CHAMPVA guide.

Other resources include this Privacy Impact Assessment, VHA Handbook 1605.04, Notice of Privacy Practices, VA privacy web site also provides a link to the VA Privacy Policy and Privacy Act Rights. Veterans also receive a notice when the visit their Veteran Affairs Medical Center (VAMC).

Section 7. Access, Redress, and Correction

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

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

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

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

As provided in the System of Records Notices (which are published in the Federal Register) 23VA10NB3 and 54VA10NB3 the location where a person may request records about themselves. First party would be a Privacy Act Request, 3rd party requests can only be processed with a signed authorization to disclose using a VHA-10-5345-REQUEST FOR AND AUTHORIZATION TO RELEASE MEDICAL RECORDS OR HEALTH INFORMATION, or a court document signed by a judge. All other request would fall under the FOIA regulation as outlined in the U.S. Department of Justice Guide to the Freedom of Information Act. VA Privacy Regulations: VA Handbook 6300.4 (Procedures for Processing Requests for Records Subject to the Privacy Act; VHA Handbook 1605.1 (Privacy and Release of Information). VA FOIA Regulation: VA Handbook 6300.3 Procedures for Implementing the Freedom of Information Act.

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.

Records in the records in the FBC archive can not be altered or updated, these records are for historical purpose only.

The System of Records Manager would facilitate the process of update their file in the System of Record which fed the records when the system was active. For beneficiaries' persons would call 1-800-733-8387. The Veteran would call 877-881-7618. Veterans would request an address change at their local Veteran Affairs Medical Center (VAMC) or calling the Health Resource Center (HRC).

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.

Beneficiaries are provided contact information when they are provided their benefits card. Also, this information is published on our web site (https://www.va.gov/communitycare/) and located in the System of Records Notice.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

The System of Records Manager would facilitate the process of update their file. For beneficiaries' persons would call 1-800-733-8387. If the Veteran is a part of Veteran Integrated Service Network (VISN) 16, the phone number is 877-881-7618. If they are calling from any other VISN, they can call the same phone number they've used previously to assist with claim/payment information. If they want to change their address, they have to do that by going to their local VAMC or calling the HRC.

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.

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 a Veteran is unaware of how to correct their information in the system.

Mitigation: FBS None. As this is a read-only historical archive, it cannot correct any information, and is only used to update the current VA information in the active non-VA Claims applications. Individuals may correct records in the System of Records which fed the records when the system was active. No updates and/or changes will be made in the archive.

Section 8. Technical Access and Security

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

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

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

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

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

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

Access is controlled by each group having access to FBCS Archive. The groups are Revenue, Clinical Integration, Appeals, Customer Service, Informatics, and Payment Operations Maintenance. All groups have User Administrators assigned which approves users for their group, and VHA has a process in place for periodic review of all users. In addition, the application has a control that removes access for an individual if they have not logged in within 30 days, and a User Administrator has to again approve a new registration each time.

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 may have access to the system and the data just as VA employees do. The services are provided under independent contracts, through OCC and the national offices. Contracts are reviewed and maintained by the contracting office and contracting officer, they are reviewed at least every two years if not more often. Privileges granted to contractors are with the approval of their supervisor or by the Contracting Officer Representative. There are no Office of Information Technology contracts in place to work on this system.

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.

In addition to the standard Privacy Awareness Training provided by the Department of Veteran Affairs, FBCS Archive also provides User Role Training and Administrator Training to all everyone requesting FBCS Archive Roles.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

A 12-month FBCS full ATO was approved 11/18/2020, which FBCA on-prim is an application. IOC for FBCS Archive s planned by 10/1/2021. The FIPS 199 classification of the system is Moderate

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

NO

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

N/A

9.3 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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.4 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.

N/A

9.5 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.

N/A

9.6 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).

N/A

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.

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2022.05.17 15:26:14 -06'00'

Privacy Officer, Michael Hartmann

Ashton Q Botts 671895

Digitally signed by Ashton Q Botts 671895
Date: 2022.05.17 15:36:46 -06'00'

Information System Security Officer, Ashton Botts or James Alden

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2022.05.18 08:10:09 -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).