Privacy Impact Assessment for the VA IT System called:

Intake, Conversion and Mail Handling Systems Upload Systems (ICMHS)/File Conversion Service (FCS)

Veterans Claim Intake, Processing, Conversion Assessing Services (VCIP) Veterans Benefits Administration VBA

Date PIA submitted for review:

11/11/2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tracy Hendrix	Tracy.Hendrix@va.gov	202-632-7704
Information System Security Officer (ISSO)	Jose Diaz	Jose.Diaz4@va.gov	312-980-4215
Information System Owner	Derek Herbert	Derek.Herbert@va.gov	202-461-9606

Abstract

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

<<ADD ANSWER HERE>>

GDIT's ICMHS/FCS (Intake Conversion and Mail Handling Services/File Conversion Services) uploads includes standard operating procedures, staff, access to VA support systems and integrated/automated IT systems which all support the upload of images, indices, and extracted metadata to VBA via VBMS (Veterans Benefits Management System) to achieve "delivery" – a term referring to the upload of data to the upload service and confirmation from that VA service that the transaction was successful. Additionally these processes and solutions provide the infrastructure that allow the CSRA-ICMHS/FCS team to meet the timeliness and quality standards required by the VBA OBPI.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The fundamental mission of the Veterans Benefits Administration (VBA) is to provide Veterans, service members, and their families the benefits they have earned through their military service to the United States. VBA accomplishes its mission by delivering client-centered, personalized services that help Veterans readjust to civilian life and enhance their well-being.

The Department of Veterans Affairs (VA) continues to optimize the Veterans Benefits Management System (VBMS), a paperless claims processing system that greatly reduces the time required to establish, develop, decide, and pay claims. The system replaces what was once a largely manual and paper-based process that had inherent bottlenecks and inefficiencies that led to processing delays and errors. Ongoing development of and continued enhancements to VBMS support VBA's progression towards an automated (or computer-assisted) processing environment. In an effort improve benefits processing efficiency and cycle-time, VBA expanded the Document Conversion services to include Intake, Conversion and Mail Handling Systems Upload Systems (ICMHS) and File Conversion Services (FCS). This effort is expected to positively impact the conversion and expedite the processing of applications of about 7.5 million veterans, whose applications are expected to be processed through the aid of this system.

ICMHS/FCS is a General Support System connected to the VA MPLS. The legal authority to design, develop, operate and manage this system is derived from the task/contract award document TAC-16-21366 and associated PWS.

The contract with AWS and CSRA state that VA is the data owner. It consists of a system component in an AWS FEDRAMP authorized GovCloud region and multiple Document Conversion sites subcontracted to Exela and Iron Mountain to form the ICMHS/FCS system boundary. These components have intersystem boundaries. The system consists of multiple virtual servers, including a database server, SFTP, API, production and preproduction servers, hosted within a Virtual Private Cloud (VPC). The system establishes a secure Checkpoint VSEC VPN gateway with VBMS on one end and the processing facilities. The interconnection with VBA is covered by an Interconnection Security Agreement (ISA-MOU).

The ICMHS activities require Document Conversion Services (DCS) conversion site to sometimes receive source materials directly from Veterans, Veterans Representatives, and third parties providing evidence in support of a claim rather than from VBA Regional Offices (RO) exclusively. Materials are received via physical mail, direct upload (by an external Veteran Service Organization user), secure file transfer, and fax. The materials are converted into searchable Portable Document Format (PDFs) which are then made available to VA end users for review within the ICMHS portal. Upon completion of regional office end user required actions, images, with associated data, are uploaded to VBMS. The DCS site then prepare source material for storage.

VBA also implemented the Private Medical Records (PMR) Retrieval Program to improve timeliness for the receipt of medical records in support of a Veterans' claim for disability benefits. The PMR program is designed to work in collaboration with the ICMHS program to support claims development. Under the PMR process, the DCS conversion vendors receive medical release statements (VA Form 21-4142, 21-4142a, and other medical release of information authorizations) via physical mail, direct upload, secure file transfer, and fax. The DCS site scan the medical release statements, convert the images to PDF format, and transfer the PDF files and metadata to the PMR

vendor via an existing secure, automated, system-to-system process. The private medical records are then requested by the PMR vendor on behalf of VA. In parallel, the DCS site upload the medical release statements to the VBMS eFolder per the existing ICMHS process.
As the work is being completed by the PMR vendor, it is securely transferred back to the DCS conversion site. The returning electronic documents include medical records / evidence received, letters, reports of contact, returned mail (in some instances), and reject notices. These are transferred back to the DCS conversion site via the secure, automated system-to-system process. Each electronic document and associated metadata received from the PMR vendor is then uploaded into the VBMS eFolder in the same manner and by the same processes as used for the documents converted by the DCS conversion vendors. If any of the documents fail to upload into the VBMS eFolder, the documents are routed through the ICMHS process and made available to VA end users for resolution. While each of the existing DCS conversion locations executes the current conversion process from receipt through storage, specific internal procedures and systems utilized are at the DCS vendors' discretion.

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.

ICMHS does not maintain PHI or PII within the system metadata. All converted data is labeled in accordance to the Document Conversion Rules provided by VA. The labels use the following identifiers and are considered VA SPI.
- Veterans Full Name
- Veteran File Number
- RMN, Records Management Number (associated with the container of source material in which the DCS is contained)

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

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

- Veteran File Number
- RMN (associated with the container of source material in which the DCS is contained)
- Document Control Sheet ID (a 14 letter/number unique identifier)
- Participant ID (a VA-assigned unique identifier for the Veteran)

PII Mapping of Components

ICMHS/FCS consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ICMHS/FCS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAPortal.com	**Yes**	**Temporarily**	**SSN, DOB**	**Digitize and transmit to VBA**	**Encrypted at rest, in transit and in process.**
FCS	**Yes**	**Temporarily**	**SSN, DOB**	**Digitize and transmit to VBA**	**Encrypted at rest, in transit and in process**

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

ICMHS receives source materials directly from Veterans, Veterans Representatives, and third parties providing evidence in support of a claim. ICMHS converts the source materials in accordance with the VA Document Conversion rules. The labels are created using the following identifiers and are considered VA SPI.

- Veterans Full Name
- Veteran File Number
- RMN (associated with the container of source material in which the DCS is contained)
- Document Control Sheet ID (a 14 letter/number unique identifier)
- Participant ID (a VA-assigned unique identifier for the Veteran)

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.

ICMHS has an MOU with VBA outlining personnel security, training, and transmission of data. VA through VBA owns all data. All privacy ICMHS supports multiple steps of the conversion process to ensure that VA receives images and data of sufficient quality to support its business processes.

Documents collected may include both printed and handwritten content from:

- paper
- photographs
- faxes

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

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

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

The major purpose for collecting the information mentioned earlier is simply to convert the documents containing such information into searchable electronic PDF format. Note however that the sensitive information are not directly collected, but could be contained in the documents accompanying benefits applications from veterans.

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

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

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

Information contained in scanned images/documents are extracted and transmitted with the scanned images to VBA. Prior to transmitting the data, it goes to through multi steps review and QA to ensure accuracy of information extracted. There is also a requirement for monthly reporting on quality to VA. The reports cover metrics, measurements, maintenance procedures among others. This is reported on monthly basis while the extraction QA is done as part of the line activities in the operations.

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

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

ICMHS has identified VA, through the issued PWS as the legal authority to operate the system and provide privacy disclosure. ICMHS has registered the system with VA and completing and maintaining Accreditation in accordance with VA Handbook 6500 and the Accreditation SOP. The authority to disclose VA data per this agreement must comply with disclosure authority under each of the below applicable statutes:

- Privacy Act of 1974, 5 U.SC. § 552a
- Confidential Nature of Claims, 38 U.S.C § 5701
- HIPAA Privacy Rule, 45 C.F.R. Part 164
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
- Confidentiality of healthcare Quality Assurance Review Records, 38 U.S.C. § 5705
- Freedom of Information Act, 5 U.S.C. § 552

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

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

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

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

The purpose of the program/system is to convert veterans' benefits applications and accompanying documents to a searchable electronic PDF format. Having the files in electronic formats expedites the benefits processing times and ultimately reduces the wait time for veterans. These source materials (documents) often contain PII and PHI. The program does not directly collect the information from veterans.

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

The information is relevant to the extent of making benefits application decision. This part, however, is entirely managed by VBA, a part of the veterans affairs. The system assigns a

unique records management number (RMN) for the purpose identifying veterans files in the system.
Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

The program does not collect information directly from individuals. The veterans send their applications and documents (source materials) to VBA who in turn send the source materials to the program for conversion and transmission purposes.

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

The extracted information forms part of the data transmitted to VBA through VBMS. These records undergo multilayered QA and verification to ensure accuracy and integrity of the records. The scanned images are in pdf format, hence protected from edits. There is also FIP 140-2 compliant encryption standards in use for the data at rest, transit and process to secure the integrity of the data.

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:
The major existent privacy risk with the information and data associated with the program/system is data loss and disclosure.

Mitigation:
PHI and PII are contained in the sourced material, ICMHS does not use PHI or PII as metadata. ICMHS limits the access to sourced material and converted data by automating the conversion process, using FIPS 140-2 encryption for data at rest and data in transit. FIPS 140-2 protocols are used to transmit data as outlined in the system description. All ICMHS personnel require a minimum NACI background investigation. Based on role and level of access a SAC may be required. Personnel security requirements for SAC are outlined in the MOU with VBA.

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.

ICMHS digitalizes source material and has quality metrics in place to ensure converted items meet VA requirements. Source Material is then sent to VA Records Management. Digitalization of sourced material reduces the overall risk to VA of maintaining sourced material at VA regional offices and provides a process for individuals to upload forms electronically to their VBMS health record.

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

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

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

The system does not create or add any new information about an individual. However, for the purpose of searching and identifying individual records, the system creates a unique RMN (Records Management Number) for individuals. This number is used to search and identify individual's record in the database and for processing.

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access

documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

PHI and PII are contained in the source materials, ICMHS does not use PHI or PII as metadata. ICMHS limits the access to source materials and converted data by automating the conversion process, using FIPS 140-2 encryption for data at rest and data in transit. FIPS 140-2 protocols are used to transmit data as outlined in the system description. All ICMHS personnel require a minimum NACI background investigation. Based on role and level of access a SAC may be required. Personnel security requirements for SAC are outlined in the MOU with VBA.

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

ICMHS retains source materials, images, and image metadata for 60 calendar days following confirmation of successful upload to VBMS. ICMHS shall store source materials onsite where document conversion occurred in conditions and security consistent to source material awaiting scanning. Storage of source materials, images, and image metadata beyond the required 60 calendar days. At the conclusion of the required 60 calendar day retention period, the ICMHS shall ship source materials to VA’s Records Management Services vendor for storage awaiting disposition.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.
The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

ICMHS/FCS retains source materials, images, and image metadata for 60 calendar days following confirmation of successful upload to VBMS. ICMHS shall store source materials onsite where document conversion occurred in conditions and security consistent to source material awaiting scanning. Storage of source materials, images, and image metadata beyond the required 60 calendar days. At the conclusion of the required 60 calendar day retention period, the ICMHS shall ship source materials to VA’s Records Management Services vendor for storage awaiting disposition.

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.

ICMHS retains source materials, images, and image metadata for 60 calendar days following confirmation of successful upload to VBMS. ICMHS shall store source materials onsite where document conversion occurred in conditions and security consistent to source material awaiting scanning. Storage of source materials, images, and image metadata beyond the required 60 calendar days. At the conclusion of the required 60 calendar day retention period, the ICMHS shall ship source materials to VA’s Records Management Services vendor for storage awaiting disposition.

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

ICMHS limits the use for SPI to the converted documents as outlined in the specifications in the PWS and the MOU with VBA. The system does not directly use SPI for processing the scanned images or documents. Files are mapped to unique Records Management Number (RMN) generated for the records.

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

ICMHS/FCS does not use PII/PHI nor SPI for research, testing and training purposes. The environment, designed to have a production and preproduction environments uses dummy data for testing and training purposes. This is intended to preserve the privacy and reduce potential risks associated with the unauthorized disclosure of the information.

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

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

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

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

<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?

The project only retains scanned images and image metadata for 60 days following successful upload to VBMS. The system does not retain the data beyond the specified timeframe.

<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?

Per the project PWS, PII/PHI (which are often contained in scanned documents) are only retained for 60 days within the ICMHS/FCS system. The project follows VA approved guidelines and the PWS specification for privacy protection.

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: Unauthorized disclosure of information

Mitigation: Scanned images are stored in database and encrypted both at rest, in transit and in process. The SPI management is in line with the PWS specifications as well as approved VA guidelines and the ISA MOU with VBA.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VBA through VBMS	VA owns the data the system generates. VBA retains the digitized data/images in VBMS.	The converted pdf/documents, images and extracted information.	FIPS 140-2 compliant protocols, HTTPS and SFTP over VA MPLS network
DAS	A part of VBA, data aids in making benefits applications processing decisions faster.	The converted pdf/documents, images and extracted information.	FIPS 140-2 compliant protocols, HTTPS and SFTP over VA MPLS network.

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: Major risk is unauthorized disclosure or access to information.

Mitigation: Use of FIPS 140-2 encryption for data at rest, in use and data in transit. Automation of the conversion process. Limit access from only approved FIPS 140-2 devices. Use of FIPS 140-2 protocols for data in transit, at rest and in use. All ICMHS portal users (external users) require PIV authentication or OTP to upload material.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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

ICMHS/FCS does not share converted documents nor any data with any external third parties or organization. Sharing is ONLY with VBA through VBMS.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: N/A, ICHMS does not share data with external organizations as referenced below in the mitigation

Mitigation: Data is not shared with external third parties. Access to the ICMHS portal for users require PIV authentication or OTP on a provisioned account. MOU with VBA outline requirements of internal users that have access to sourced material. DCS and ICMHS AWS workloads have a separate internal system boundary reducing access in each environment. PWS outlines the specification for sourced material and automated process and include quality, verification and reporting requirements.

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.

ICMHS/FCS does not collect personal or personal health information nor SPI from individuals. However, as mentioned earlier, benefits application documents, which are the source materials being converted, extracted and transmitted to VBA through VBMS may contain PII and/or PHI. The requisite notice is provided by VBA which is responsible for collected the information from individuals. The project PWS empowers the system to receive the source materials from the VA or the storage facilities.

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

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

The ICMHS/FCS system does not directly receive nor collect SPI from individuals. They are sent to VBA directly. The discretion to either provide or decline to provide PII/PHI is determined between the veteran and VBA.

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

This system is limited to document conversion and image data transfer to VBA through VBMS. The right to consent to any use of information is determined by VA (VBA) and retains the responsibility to notify the individuals or information owners.

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

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

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

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

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

Follow the format below:
<u>Privacy Risk:</u> Possible unauthorized access, use or disclosure of personal information.

<u>Mitigation:</u> The system does not directly collect personal information from veterans. The system only scans, converts and extracts information from source materials. These source materials however might contain personal information. The responsibility for notice issuance lies with VBA. The system does not make use of, nor share individuals' information for any purpose. A unique Records Management Number (RMN) is generated by the system and assigned to individual records.

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.

The ICMHS/FCS system is not a public facing application or system. Access is role based for business need purposes only. Individuals' access to their information will be directly channeled to VBA systems.

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.

ICMHS/FCS does not collect veterans' information, Source materials often contain these information and are scanned as is. If there is need for individuals to correct their information, that request or process is managed by VBA.

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.

Since the VBA collects these information, there will also be a means of notifying individuals of any need make corrections in their information. This is outside the scope of the system.

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.

This is outside the scope of the system. VBA would have a means of letting individuals/veterans correct or update their information.

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: This is not applicable to the system, for the reasons stated in the mitigation statement below.

Mitigation: This is not directly applicable to the system in review. The circumstances and need for correcting, updating or removing any information is determined by VBA.

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.

Access to the ICMHS/FCS is role based and strictly on need to know. Access is granted to VA-cleared, PIV issued personnel with role-based need.

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?

Users are either GDIT program team with functional need or VA/VBA personnel with functional need to know.

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.

The roles are determined by individual's functional need. Enough access is granted just to achieve specific tasks.

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

Access to the ICMHS/FCS is role based and strictly on need to know. Access is granted to VA-cleared, PIV issued personnel with role-based need. Users are either GDIT program team with functional need or VA/VBA personnel with functional need to know. The roles are determined by individual's functional need. Enough access is granted just to achieve specific tasks.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

ICMHS/FCS is developed and managed by GDIT, a VA contractor as a SaaS system. There is a Confidentiality agreement as well as NDA, ISA-MOU defining the parties' scope and functions.

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.

Users are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training on VA TMS platform. There is also a GDIT provided recurrent training for system users.

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

Yes

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted, (*(**Granted on 9/21/2020**)
2. *Whether it was a full ATO or ATO with Conditions,* (**Granted with conditions**)
3. *The amount of time the ATO was granted for, and* (**120 days**)
4. *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.

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

<<ADD ANSWER HERE>>

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Tracy M Hendrix 1466255

Digitally signed by Tracy M Hendrix 1466255
Date: 2020.12.07 12:09:26 -05'00'

Privacy Officer

Jose Diaz 386249

Digitally signed by Jose Diaz 386249
Date: 2020.12.07 09:39:58 -06'00'

Information Security Systems Officer

DEREK L. HERBERT 312060

Digitally signed by DEREK L. HERBERT 312060
Date: 2020.12.04 15:17:39 -05'00'

System Owner

APPENDIX A-6.1

PRIVACY NOTICE PROVIDED TO USERS PRIOR TO LOGGING INTO THE SYSTEM:

WARNINGWARNING**WARNING**

You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following:

•You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transferred or stored on this information system.

•Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose. For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

-