SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=767&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Signature Informed Consent (SIC) – iMedConsent Web (ICW)

VHA National Center for Ethics in Health Care (NCEHC)

Date PIA submitted for review:

27 April 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Nancy Katz-Johnson*	*Nancy.katz-Johnson@va.go*	*(203) 535-7280*
Information System Security Officer (ISSO)	*Richard Alomar-Loubriel*	*Richard.Alomar-Loubriel@va.gov*	*(787) 696-4091*
Information System Owner	*Larry Carlson*	*Larry.carlson2@va.gov*	*(509) 466-2103*

Abstract

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

The Signature Informed Consent – iMedConsent Web software is a cloud-based solution to integrate informed consent into the electronic medical records process and reduces the incidence of lost and misplaced forms. This software solution improves patient safety by decreasing delayed or postponed procedures and is used in all medical centers and Community-Based Outpatient Clinics (CBOCs).

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?*

Signature Informed Consent(SIC) is now iMedConsent Web (ICW) and is the new software system being interfaced with VistA via the VA Enterprise Cloud (VAEC) at the request of the National Center for Ethics in Health Care (NCEHC) program office.

This solution was placed under contract to provide a single, web-based software solution to allow clinicians to meet obligated ethical standards of practice required by law, regulation, and policy that require VHA to obtain patients' signature informed consent (see The Joint Commission Standard RI.2.4.0, VHA Handbook 1004.1, Title 38 CFR § 17.32, and Title 38 USC 7331). VHA implementation of these policies and this program are managed by NCEHC to support the VA's requirement to provide highly ethical, patient centered informed consent processes.

This software will be used to store the proprietary content library, licensed with iMedConsent, for signature informed consent forms and subsequently signatures for acknowledgement for approximately 3,300,000 forms annually. All of these forms will contain patient information and are immediately sent as a file to VIX/CAMMS (written) to Vista or Cerner. Signature informed consent is obtained for all invasive medical procedures and all higher risk medical treatments (e.g., all surgeries, all allergy testing, all administration of long-term opioid therapy for pain).

ICW software will be deployed using an enterprise license and will be used by virtually every provider in the VHA health care system, nationwide.

The information documented includes patient identifying information (name, SSN, possibly date of birth) along with information on the treatment that is being consented to. The system may be used to complete other administrative forms such as Release of Information and Leaving Against Medical Advice forms.

The information generated by this system is shared with the Computerized Patient Record System (CPRS), VistA Imaging Exchange (VIX), and the Cerner Millennium electronic health record (EHR).

The system is accessed by all VHA sites that have access to the EHR. There is only one national iMedConsent™ library of forms, which is accessed by all sites. This helps maintain continuity of content and consistency of documentation across sites.

ICW has achieved an Authorization to Operate (ATO).

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

The system does not require a System of Records Notice (SORN) as the system is not a SOR. The record copy of all documentation processed by this system is the existing EHR (CPRS using VistA Imaging or Cerner via Powerchart/CareAware MultiMedia (CAMM) Vendor Neutral Archive.

The system uses cloud technology (VAEC Microsoft Azure GovCloud (MAG)). The system is hosted in a Federal Risk and Management Program (FedRAMP) Cloud Service Provider that has a PIA to cover the infrastructure and has an ATO with the VA.

The PIA for the Cloud Service Provider delegates ownership of data to the system owner and states that the customer is responsible for their system's data, including PII

The VA owns all ICW data and there is a Business Associate Agreement (BAA) with the Cloud Service Provider, Contractors or VA Customers establishing different ownership rights.

If privacy related data is disclosed, intentionally or unintentionally, there would be serious harm to the reputation of VHA as a premier provider of health care, as well as the possibility of harm to the security of the identity of veterans impacted by any such breach.

Section 1. Characterization of the Information

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

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

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

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

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

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

Provider ID#

PII Mapping of Components

ICW consists of two (2) key components. Each component has been analyzed to determine if any elements of that component collects PII. The type of PII collected by ICW and the reasons for the collection of the PII are in the table below. It should be noted that nothing is directly collected by ICW apart from signatures.

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
Azure SQL via JumpServer in VAEC	Yes	*Yes*	• *Name* • *SSN* • *Date of Birth* • *Address* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number*	Ensure proper patient selection for use by application	Read only information for the user. Data encrypted at rest

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.

ICW pulls names, dates of birth, and SSNs from an interface with the VA's Master Person Index (MPI). The interfaces are needed to be to pull this data in a formatted setup for validation with systems the completed forms are sent to (e.g. Cerner, VistA, VistA ImagingMPI).

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.

ICW software collects PII via electronic interfaces with the Master Person Index (MPI), including the Centralized VistA Imaging Exchange (CVIX), Application Programming Interfaces (APIs), and with Cerner, Fast Healthcare Interoperability Resources (FHIR) APIs.

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

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

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

The data is used to validate patient identification linked to the presented consent form for clinical treatments and procedures. The procedure information used is needed to ensure patient understanding of the treatment plan that they are consenting to.

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.

The data is not checked against any other source of information and is not used to make decisions about an individual. The MPI is the authoritative patient data source.

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

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

Title 38 U.S.C. § 7331, Title 38 U.S.C. 7332, and Title 38 CFR Section 17.32

1.7 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: Loss of Privacy Data. ICW handles PII information and there is a risk that the information may be improperly accessed or defaced, though the risk is mitigated by the control of the access being limited to the users of the VA's EHR and its operating locations within the VAEC MAG.

Mitigation: ICW takes a defensive, in-depth approach to protecting patient PII data to include the following protection mechanisms:

1. The Application's Programming Interface (API protected by a policy enforcement/policy decision point
2. VA hosts in MAG are protected by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services.
3. Data -at-rest encryption for any partition where PII will be contained

4. Data -in-transit encryption on any network traffic beyond the local enclave

Section 2. Uses of the Information

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

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

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

The information will be used to document both providers' and patients' electronically captured signatures for informed consent for all treatments and procedures requiring signature in accordance with VHA Handbook 1004.01, Informed Consent for Clinical Treatments and Procedures.

Name – pulled in for identify verification

SSN –pulled in for identify verification

Date of Birth – pulled in for identify verification

Address – pulled in for identify verification

Procedure/treatment description – provided as templates in ICW, linked to patient and provider to obtain patient consent (signature) for treatment

Identifiers such as visit information and medical record number – pulled in for compilation/verification as well as capturing the signatures.

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

ICW logs usage information on the signature informed consent forms that are produced. This data is ingested into SQL servers for historical analysis, reporting for quality improvement measures, and usage analysis. The data is not placed in the individual's existing record.

2.3 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.

The minimum-security requirements for ICW cover the security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.

The MAG FedRAMP High ATO package employs security controls in the respective HIGH impact security control baselines unless specific exceptions have been allowed based on the tailoring guidance provided in VA agency high ATO for Microsoft Azure and NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

The only access to ICW is though the electronic health record, and the inherited training requirements for CPRS/VistA access or access granted by Cerner, meet the training needs for the ICW as well, requiring annual completion of Talent Management System (TMS) courses on Information Security and Protecting PHI/PII, along with the requirement to review Rules of Behavior.

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

The patient name and SSN information are retained by the system along with the name of the associated signature informed consent document completed; all in accordance with VA audit requirements and is retained for analysis and reporting.

Non-record copy, signature informed consent forms are stored for 60-days before auto-deletion. This is to allow for completion of incomplete forms and for forms review as needed in the event of unanticipated networking outages, communication loss, VistA Imaging or Cerner downtime(s).

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.

Given that ICW is not a system of record, the consent form will be returned or destroyed upon completion of the applicable contract or agreement. Data resides in ICW for 60 days, to fulfill the specified contract, clinical, or administrative need as well as to ensure full write to EHRs. VHA Handbook 1004.05 *iMedCONSENT™* (https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3064) and 1004.01 *INFORMED CONSENT FOR CLINICAL TREATMENTS AND PROCEDURES* (https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2055) control and define this time period. Once the consent form is transferred to the authoritative EHR system, that system's record retention schedule goes into effect.

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.

After 6o days, the consent form is removed from ICW and will be maintained per the schedule of the EHR it is transferred to.

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

Procedures include the DoD approved wiping of any media that contains PHI or PII and properly disposed of using data destruction services in accordance with VA 6500. Data destruction procedures are outlined in the Infrastructure Operations Manual in accordance with VA Directive 6500 - Media Sanitization Guideline and NIST 800-88 Media Sanitization.

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

ICW data is not used in research. "Live" data is never used in testing or training. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords, access for need to know basis, Active Directory, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN) are utilized.

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

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

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

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

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

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

Follow the format below:

Privacy Risk: ICW handles PII information and there is a risk that the information may be improperly accessed or defaced, though the risk is mitigated by the control of the access being limited to the users of the VA's EHR's. The longer the time frame that information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation: Data retention procedures are enforced through strict physical and logical access controls that include limited physical access to any VA system, complete inventory of all systems, and auditing of system or file status to ensure changes to a system status, (i.e. going offline for destruction, removal of file being wiped) is enforced by notifying appropriate personnel as well as maintained for auditing and establishing a timeline of events. Records are only retained for 60 days and then deleted following the steps in 3.4

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***
MPI	Ensure proper patient selection for use by application, Quality Control and Quality Improvement to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Name* • *SSN* • *Date of Birth* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections
CDW	Ensure proper provider selection for use by application to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Provider Name* • *Provider emailIdentifiers such as VA provider number*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections
VistA Imaging Exchange (VIX)	Ensure proper patient selection for use by application, to pass note and consent to VIX	• *Name* • *SSN* • *Date of Birth* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections

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***
Clinical Content Object Workgroup (CCOW)	Ensure proper patient selection for use by application, to keep the proper patient in context to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Data File Number (DFN)* • *Station ID* • *Vault for Station ID*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections
Active Directory (AD)	Ensure proper user authorized for use of the application, and establish their permitted role within the application to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Name* • *Universal Person Identifier (UPN)* • *VA email address* • *VA email address* • *provider number*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections
Single Sign-On Internal (SSOi)	Ensure proper user authentication for use by application, Quality Control and Quality Improvement to ensure required use of the software IAW VHA Handbook	• *Uniform Resource Locator (URL) exchange between the systems* • *ID sent to ICW*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections

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*
	1004.05 and 1004.01		
EHRM	Ensure proper patient selection for use by application, Quality Control and Quality Improvement to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Name* • *SSN* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number or EDIPI (Electronic Data Interchange Personnel Identifier)*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections
CPRS	Ensure proper patient selection for use by application, Quality Control and Quality Improvement to ensure required use of the software IAW VHA Handbook 1004.05 and 1004.01	• *Name* • *SSN or last 4* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number*	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections

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: There is risk to the organization (VAEC or DHA) that a breach could occur leading to potential identity theft or unauthorized changes to the data.

Mitigation: Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN) are utilized.

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***
Defense Health Agency (DHA) via Cerner	Allow consent and treatment information between DHA and VA	• *Name* • *SSN* • *Date of Birth* • *Address* • *Procedure/treatment description* • *Identifiers such as visit information and medical record number*	National ISA between DHA and VA	HTTPS over port 443, and encrypted end-to-end, per VAEC/CSOC boundary protections

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

Access controls, audit and accountability, awareness and training, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, media protection, personnel security, physical and environmental protection, risk assessments, system and services acquisition, system and communication protection, system and information integrity, planning, and maintenance are used to meet the requirements of OMB Memoranda M-06-15 and M-06-1.

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: The same risk of occurrence due to theft or destruction exists, but is assumed at the national level under the MOU/ISA between DHA and VA.

Mitigation: Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN) are utilized.

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.

ICW is not the SOR and as such does not collect PII data. This is accomplished by a VA EHR not ICW. In addition, this PIA serves as a form of notice.

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

ICW is the system used to collect the patient's consent for treatment. The patient's information is pulled from authoritative sources and is not changed within ICW, but the patient can refuse to sign

until the electronic record is corrected. The use of hardcopy consent with wet signature can also be used if no other option is available.

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

ICW is not the SOR and does not manage the PII or correction thereof. This is accomplished by a VA EHR not ICW.

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 individuals are unaware of their information being collected.

Mitigation: All PII information ICW collects comes directly from the EHR. ICW is not the point of collection and all information related to notice is covered in the source system(s) PIA. 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.

. Individuals gain access to their information through the release of information process related to the EHR, handled by the provider's office staff at reception/check-in, not ICW. No intake of PII occurs within ICW.

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.

ICW is not the SOR and as such does not correct data. This is accomplished through actions associated with the VA EHR not ICW.

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.

ICW is not the SOR and as such does not correct data. This is accomplished through actions associated with the VA EHR not ICW.

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.

ICW is not the SOR and as such does not correct data, nor is it the system to afford the redress. This is accomplished through actions associated with the VA EHR not ICW.

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 inaccurate information is provided by an individual and they are unaware of how to correct it.

Mitigation: All PII information ICW processes comes directly from the EHR. ICW is not the point of collection and all information related to access, redress, and correction is covered in the source system(s) PIA. 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.

ICW access is governed by the roles established for the VA staff who have access to a VA EHR. Access to ICW is also permitted to those entrusted by additional role definition to support the system. This includes VA staff, VAEC, and Taylor Communications (covered by BAA) acting in the capacity of software support. All elevated roles are assigned based on the requisite background screening and role assignment qualification which affords PIV, VistA/CPRS, or Cerner access and conjoined with Active Directory. ICW authenticates the requests made to it through coded rules that interpret the aforementioned qualifications.

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.

Tier 3 support and software operations in Azure, are provided by Taylor Communications either as needed (Nessus remediations) or on demand from a VA tier 2 request. The access to provide the support is done through role assignment (Active Directory, etc.…), PIV, zero tokens, and protected by the BAA between the parties. Taylor Communications may also provide support to the software, but through the controls of VAEC and the previous AD assignment. The Contracting Officer and Federal Acquisition Regulation (FAR) govern the term of the BAA and its subsequent renewal as well as any required reviews. FAR also governs nondisclosure.

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.

ICW will "inherit" the rules established through VA Directive 6300 and VA Handbook 6500. Training for VA employees is managed through the TMS and includes the Annual Security Awareness and HIPAA/Privacy training. Taylor Communications trains its employees annually on Fraud, Waste, and Abuse, Data Privacy, and Healthcare compliance. Taylor employees, with elevated privileges to maintain the system, do so with VA issued tokens and equipment, and are subject to the Annual Security Awareness and HIPAA/Privacy training in order to maintain their VA accounts. Background checks/Clearance levels to receive their VA tokens and equipment are performed per contract requirements by VA personnel.

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

If Yes, provide:

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

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

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

Yes,

1. *The Authority to Operate (ATO) was granted on 22 Oct 2020.*
2. *It is a Full ATO*
3. *The amount of time the ATO was granted for is 360 days.*
4. *The FIPS 199 classification of the system is MODERATE.*

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.

Nancy E Katz-Johnson 206244

Digitally signed by Nancy E Katz-Johnson 206244
Date: 2021.05.27 08:12:17 -04'00'

Privacy Officer, Nancy Katz-Johnson

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2021.05.19 15:32:04 -04'00'

Information Security Systems Officer, Richard Alomar-Loubriel

Larry E. Carlson 382018

Digitally signed by Larry E. Carlson 382018
Date: 2021.05.19 10:19:48 -07'00'

Information System Owner, Larry Carlson

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

https://www.oprm.va.gov/privacy/pia.aspx