Privacy Impact Assessment for the VA IT System called:

Insurance Capture Buffer Web (ICBWeb)

Veterans Health Administration (VHA)

eBuisness Solutions

eMASS ID #843

Date PIA submitted for review:

August 8, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Akeel Omari	Akeel.Omari@va.gov	404-828-5507
Information System Security Officer (ISSO)	Gerry Ambalada	gerry.ambalada@va.gov	(206)764-2687
Information System Owner	Tony Sines	tony.sines@va.gov	316-249-8510

Abstract

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

Insurance Capture Buffer Web (ICBWeb) is a web-based insurance card scanning and VistA Buffer File update management system designed to enhance the insurance data collection and verification processes for Veterans Affairs Medical Centers. ICBWeb is integrated with several VistA components such as, Appointment Scheduling and the Patient's Insurance File. ICBWeb provides an electronic list of veterans with scheduled appointments whose insurance needs to be verified. The "Patient Update" List is used by check-in and registration clerks to scan insurance cards for those identified. Scanned images are stored and are immediately accessible to verification clerks via the "Insurance Buffer Entries" list. Data from the image can be compared with existing insurance data within VistA. A reporting utility is available to Business Office Managers to ensure compliance of check-in and verification clerks. By expediting the data collection process at check-in, ICBWeb helps a VA facility improve the patient check-in experience and customer satisfaction. It also increases data accuracy and allows for standardization of the verification process.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*
Insurance Capture Buffer Web (ICBWeb); eBusiness Solutions, Office of Finance

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

Insurance Capture Buffer Web (ICBWeb) is a software application that assists with the collection and verification of 3rd party insurance information to support VHA Revenue Operations for Medical Care Collection Fund (MCCF) and non-MCCF 3rd party billing and collections. The VHA Office of Finance program office both owns and manages ICBWeb a nationally deployed system covering all VA Medical Centers and points of care where VistA is also available.
All PII collected and accessible in ICBWeb is saved in VistA. As such, VistA's consistency checking, and protection of patient data is used across all sites. The information used in the ICBWeb system is Veteran insurance information such as the same information that is contained on a medical insurance card. This information is collected at the VA Medical Center's clinic where the veteran has an appointment. Once the insurance card image is collected through the Entry Clerk's "patient update" module, the individual's insurance information is verified by VA employees in the Insurance Buffer module before the verified information is entered into VistA under the patient's insurance record.

ICBWeb does not contain any databases of individually identifiable information as all information collected by the program is processed to be saved in the official VA system of record; VistA. As such, there is not estimate of the number of individuals whose information is stored in the system. Selected pieces of a Veteran's VistA information and VA employee information (saved by VistA) is available for viewing using ICBWeb but is stored in VistA.

ICBWeb has the legal authority to operate under Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10), Title 38, United States Code, section 7301(a) >>

C. *Who is the owner or control of the IT system or project?*
VA Owned and non-VA Operated

2. Information Collection and Sharing

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

ICBWeb is a graphical user interface (GUI) over VistA. VistA stores the individual information for Veterans registered in a VA Medical Center to include scheduled appointments and health insurance information. This information is available in ICBWeb. ICBWeb does not contain any databases of individually identifiable information as all information collected by the program is processed to be saved in the official VA system of record; VistA. Selected pieces of a Veteran's VistA information and VA employee information (saved by VistA) is available for viewing using ICBWeb but is stored in VistA.

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

ICBWeb is a web based application (hosted on central VA Gov Cloud connected to each VistA). The purpose of ICBWeb is to streamline the collection and verification of medical insurance information for the VA Veteran population. VA medical facilities and Consolidated Patient Account Centers (CPAC) use ICBWeb to update the Veteran's official patient record in VistA. Complete and accurate administrative and demographic data is a key component of establishing and managing a patient's record in support of the VHA revenue operations collection.

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

ICBWeb is a graphical user interface (GUI) over VistA. VistA stores the individual information for Veterans registered in a VA Medical Center to include scheduled appointments and health insurance information.

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

All PII collected and accessible in ICBWeb is saved in VistA. As such, VistA's consistency checking, and protection of patient data is used across all sites.

3. Legal Authority and SORN

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

ICBWeb has the legal authority to operate under Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10), Title 38, United States Code, section 7301(a).

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

The system of record is not in the process of being modified and has an existing SORN.

4. System Changes

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

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

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

Completion of this PIA will not result in any technology changes

Section 1. Characterization of the Information

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☐ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers

☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements used: Veteran employment information and information accessible from ICBWeb is generated from VistA Patient Scheduling and VistA Integrated Billing package.

PII Mapping of Components (Servers/Database)

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Microsoft Azure Government	Yes	Yes	Name, Health Insurance Beneficiary Numbers Account numbers	Electronic Health Records	National Institute of Standards and Technology (NIST) controls in place

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information collected, maintained, and/or disseminated in ICBWeb comes from a few areas depending on the type of information. The information may come directly from Document Storage Systems, the vendor built the ICBWeb application, or the VHA Office of Finance who owns and manages the ICB system on the VA side.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information from sources other than the individual is not required.

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

The ICBWeb system uses statistics and analysis to create 3 types of general reports that provide the VA with a better understanding of revenue generating opportunities and training needs.

These are reports are:

1. Exception Reports created to analyze missed insurance collection opportunities.
2. Reports created to analyze the total number of insurance buffers collected for both entry clerks and verification clerks. This report includes the ability to drill down to specific clinic locations and individual user entries.
3. Reports created to analyze insurance collection data to track and trend user productivity.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Veteran insurance card information is collected directly from patients by VA employees, using electronic image scanners that are connected to the VA employee's workstation.

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

Paperwork is done electronically.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

All the insurance information collected from veterans is vetted through VA employees with the role of insurance verifier, who contacts the veteran's insurance companies and confirms that the insurance information is active and accurate. Once the information is verified, it is updated in the veteran's VistA insurance records. VistA is always the main source of record.

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

All the insurance information collected from veterans is vetted through VA employees with the role of insurance verifier, who contacts the veteran's insurance companies and confirms that the insurance information is active and accurate. Once the information is verified, it is updated in the veteran's VistA insurance records. VistA is always the main source of record.

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

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

ICBWeb has the legal authority to operate under Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10), Title 38, United States Code, section 7301(a).

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: The Veterans Health Administration (VHA) employ a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the patient during appointments and in other forms of communication	Internal
Social Security Number	Used as a patient identifier and as a resource for verifying income information with the Social Security Administration	Internal

Date of Birth	Used to identify age and confirm patient identity	Internal
Mailing Address	Used for communication, billing purposes and to calculate travel pay	Internal
Zip Code	Used for communication, billing purposes, and to calculate travel pay	Internal
Phone Number(s)	Used for communication, confirmation of appointments and to conduct telehealth appointments	Internal
Health Insurance Beneficiary Account Numbers	Used to communicate and bill third-party health care plans	Internal
Employment Information	Used to determine potential employer's insurance eligibility and for veteran contact, financial verification	Internal
Gender	Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual	Internal
Patient ID	Used to help identify the specific patients outside of SSN, and DOB. This ensures we have the correct patient and eliminated cross or duplicated information	Internal

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

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

The ICBWeb system uses statistics and analysis to create 3 types of general reports on ICBWeb VA employees and contractors that provide the VA with a better understanding of revenue generating opportunities and training needs. These are reports are:
1. Exception Reports created to analyze missed insurance collection opportunities.
2. Reports created to analyze the total number of insurance buffers collected for both entry clerks and verification clerks. This report includes the ability to drill down to specific clinic locations and individual user entries.
3. Reports created to analyze insurance collection data to track and trend user productivity.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

ICBWeb does not create nor store any reporting analysis on individual VA patient information.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

We use hardware encryption for all data / systems utilizing FIPS 140.2 compliant algorithms for data at rest. All data in transit is encrypted with the most recent TLS 1.2 or higher as of right now.

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

The system does not collect, process, or retain Social Security Numbers so no additional protection beyond that for the entire system is required.

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

PHI and PII are stored on encrypted volumes with field level security in the DB and TLS for all connections.

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

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

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

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

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

2.4a How is access to the PII determined?

All ICB user roles (Entry clerk, Verifier, Verifier Plus, Admin, and Admin IRM) perform insurance collection and verification processing using information collected in VistA. Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. VA OIT implements data protection assurances on all databases where patient insurance information is stored. Limited system access is granted by VA OIT to ensure only those with need to know have access to any patient related data. VA OIT periodically audits user accounts and removes access to those who no longer need access or have not used granted access in the previous audit period. All data collected, generated and stored by ICBWeb is the properly of VA and only used in VA controlled space.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes. User manuals and job aides are available.

2.4c Does access require manager approval?

Yes

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

Yes, reports are available to identify all action(s) taken on a Veteran/Patient insurance file. VistA is the system of record for PII data. Annual supervisor reviews are performed for VistA access monitoring.

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

System Administrator(s)

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name
Employment Information
Date of Birth
Social Security Number (SSN)
Race/Ethnicity
Phone Number(s)
Mailing Address
Zip Code
Health insurance account number(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.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

ICBWeb retains Veteran insurance card image for 13 months.
• RCS 10-1 link for VHA: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

• National Archives and Record Administration: http://www.nara.gov

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

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

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

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

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

ICBWeb retains Veteran insurance card images for 13 months and follows Schedule (RCS) 10-1, Destroy/delete when no longer needed for administrative or clinical operations, N1-15-02-3, item 3.
• RCS 10-1 link for VHA: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

• National Archives and Record Administration: http://www.nara.gov

3.4 What are the procedures for the elimination or transfer of SPI?

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

ICBWeb's main system of record is VistA, Information within the VISTA system is destroyed by the disposition guidance of the RCS 10-1; maintain records for 75 years. The VISTA system was implemented in the 1970's and the SPI contained within the system will not be ready to destroy or dispose of until the 2040's. On or before that time, VHA Records Management and Office of Information Technology will develop a plan for disposal or deletion. The plan will be routed for approval and implementations through VHA, Veterans Administration Central Office and the National Archives. "Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

https://www.va.gov/vapubs/search_action.cfm?dType=1.

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

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

ICBWeb uses existing TEST patient data already available in field VistA locations. TEST Patient data entered and utilized conforms with:

- VHA Directive 1906 - https://vaww.va.gov/vhapublications/viewpublication.asp?pub_id=11388
- VHA Directive 1604 - 1906_D_2020-04-10 pdf

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

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained for ICBWeb could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, the ICBWeb adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI).”

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA VistA System(s)	Patient Insurance information is integral to VistA's Integrated Billing and Revenue Operations	VistA's Patient Insurance Type sub-file	Electronically: saved in VistA
VA Enterprise Cloud Microsoft Azure Government Cloud	Copies of Patient Insurance cards is integral to ensuring accurate information is entered and maintained in VistA Integrated Billing package	Insurance Card Images	Securely transmitted by application front end to VA EC MAG only. Not shared with other applications or entities

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information or data may be shared with unauthorized VA program or system.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities

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.

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

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

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

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

Data Shared with External Organizations

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is no external sharing.

<u>Mitigation:</u> There is no external sharing.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

VHA provides notice of information collection in several ways. The initial method of notification is in person during check-in at the individual's appointments or in writing via the Privacy Act statement on forms and applications completed by the individual. All VA Medical Centers post large posters of the Privacy Act statements supporting the collection, use and maintenance of PII and PHI by VA. In addition, information disclosure is required by law as published in 38 United States Code (U.S.C.) 7301 (b). Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES

- Applicants for Employment under Title 38, USC-VA, SORN 02VA135 (prior to 1995)
- Individuals Serving on a fee Basis or Without Compensation (Consultants, Attending, and Others or paid Indirectly through a Disbursement Agreement) Personnel Records–VA, 14VA05 / 75 FR 70778
- Accreditation Records-VA, 01VA022 (Consolidated), 12/20/2013
- Individual Correspondence Records-VA, 05VA026 / 73 FR 72121/ 11/26/2008
- Employee Medical File System Records (Title 38)-VA, 08VA05 / 88 FR 4885, 1/25/2023
- Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations-VA, 09VA05 / 88 FR 4885, (Published Prior to 1995)
- Patient Advocate Tracking System Replacement (PATS-R)-VA, 100VA10H / 86 FR 6988, 1/25/2021
- Professional Standards Board Action and Proficiency Rating Folder (Title 38)-VA, 101VA05 / 65 FR 45137, 7/20/2000
- Agency-Initiated Personnel Actions (Title 38)-VA, 102VA05 / 65 FR 46551, 7/28/2000
- Police and Security Records-VA, 103VA07B / 89 FR 23638, 4/04/2024

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

Reference 6.1a

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Reference 6.1a

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

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

Yes, individuals do have an opportunity to decline to provide information at any time. No, there is not a penalty or denial of service for declining to provide information.

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.

Individuals have the right to consent to particular uses of information. Individuals are directed to use the 10- 5345 Release of Information form describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of 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 veterans and other members will not know that the VHA Office of Finance exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The VHA Office of Finance mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1 VHA Notice of Privacy Practices

Section 7. Access, Redress, and Correction

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

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

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

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

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the myHealthevet program, VA's online personal health record. For more information about myHealthevet, please visit https://www.myhealth.va.gov/index.html
In addition to the procedures discussed above, the SORNs listed in question 6.1 each address record access, redress, and correction. Links to all VA SORNs can be found at https://www.oprm.va.gov/privacy/systems_of_records.aspx

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

Reference 7.1a

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

Reference 7.1a

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.

Individuals are provided the opportunity to submit a request for change in medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer (PO), or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing.

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.

The SORNs listed in question 6.1 each discus and notify members of the public of the procedures related to record access, redress, and correction. Links to all VA SORNs can be found at: https://www.oprm.va.gov/privacy/systems_of_records.aspx

Individuals may request correction of their information by contacting a Medical Support Assistant, the Chief of Health Information Management Systems (HIMS), the Patient Advocate and or the Release of Information Office (ROI).

Individuals are provided verbal notice of amendment process by the PO and/or HIMS Chief at time of request.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A formal redress process via the amendment process is available to all individuals. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record, a veteran or other VAMC patient who is enrolled in myHealthevet can use the system to make direct edits to their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals whose records contain incorrect information, the Veteran's Administration may not receive financial compensation for services rendered

Mitigation: The VHA Office of Finance mitigates the risk of incorrect information in an individual's records by authenticating information when possible using the resources discussed in question 1.5. Additionally, VHA Office of Finance staff verifies information in insurance records and corrects information identified as incorrect after patient appointments.

Additionally, VA staff is informed of the importance of maintaining compliance with VA Release of Information (ROI) policies and procedures and about the importance of remaining alert to information correction request

Section 8. Technical Access and Security

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

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

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

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

Individuals receive access to the ICBWeb system by gainful employment in the VA or upon being awarded a contract that requires access to ICBWeb systems. Upon employment, the Office of Information & Technology (OIT) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. Veterans Health Administration (VHA) Supervisors are required to review and approve an individual's initial and additional requests for access. Approval process is documented and maintained by the Information Technology (IT) office and the Information Security Officer (ISO).

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

No user outside of ICBWeb have access to ICBWeb system.

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

All ICB user roles (Entry clerk, Verifier, Verifier Plus, Admin, and Admin IRM) perform insurance collection and verification processing using information collected in VistA.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, contractors will have access to the ICBWeb system. Contracts are reviewed annually by the Contracting Officer Representative (COR). Clearance levels are determined by the COR and position sensitivity level and risk designation. Access is reviewed annually, and verification of annual Privacy and Information Security Training and VA Rules of Behavior signatures are validated by the COR. All contractors must abide by the following contract terms and conditions included by reference in their contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All users of the ICBWeb system are required to complete annual privacy and information security training, as well as to read and agree to VA Rules of Behavior.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 09/05/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11/15/2023
5. *The Authorization Termination Date:* 11/14/2025
6. *The Risk Review Completion Date:* 11/13/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

Reference 8.4a

Section 9 – Technology Usage

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

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

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

ICBWeb operates in the cloud utilizing VA Enterprise Cloud (VAEC) / Microsoft Azure Government (MAG) Platform as a Service (PaaS)

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in

the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?
This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

AKEEL OMARI Digitally signed by AKEEL OMARI
Date: 2024.09.30 11:18:44 -04'00'

Privacy Officer, Akeel Omari

GERARDO AMBALADA Digitally signed by GERARDO AMBALADA
Date: 2024.09.30 11:21:52 -07'00'

Information Systems Security Officer, Gerry Ambalada

TONY SINES Digitally signed by TONY SINES
Date: 2024.09.30 13:54:51 -05'00'

Information Systems Owner, Tony Sines

APPENDIX A-6.1

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

VHA Notice of Privacy Practices

HELPFUL LINKS:

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

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

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

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

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