Privacy Impact Assessment for the VA IT System called:

Electronic Health Record Modernization (EHRM) Audiology Workstations System (EHRM AUDIO)

Electronic Health Record Modernization Integration Office (EHRM IO)

Office of the Deputy Secretary of VA (DEPSECVA) - VA Central Offices (VACO)

Date PIA submitted for review:

June 2, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.Siefert@va.gov	202-632-8430
Information System Security Officer (ISSO)	Jeramy Drake	Jeramy.Drake@va.gov	509-956-8865
Information System Owner	Michael Hartzell	Michael.Hartzell1@va.gov	803-406-0112

Abstract

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

The Electronic Health Record Modernization (EHRM) Audiology Workstations system is an End User Device (EUD) system consisting of the standard Department of Veterans Affairs (VA) Enterprise Windows 10 desktop image. This standard Windows 10 desktop image is the foundational platform that hosts various clinical audiology applications and tools dedicated to support the delivery of health care throughout the Veterans Health Administration (VHA) operating environments such as VA medical centers (VAMCs) 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.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

For better technical and functional management purposes, the EHRM Audiology Workstations system boundary has been formed as part of a de-coupling effort of the EHRM Multi-Purpose Clinical Platform (M-PCP). The system is owned by the VA Electronic Health Record Modernization Integration Office (EHRM IO), which reports directly to the Office of the Deputy Secretary of VA (DEPSECVA). EHRM Audiology Workstations is an End User Device (EUD) enterprise system consisting of the standard Department of Veterans Affairs (VA) Enterprise Windows 10 desktop image. This standard Windows 10 desktop image is the

foundational platform that hosts various clinical audiology applications and tools dedicated to support the delivery of health care throughout the Veterans Health Administration (VHA) operating environments such as VA medical centers (VAMCs) and community-based outpatient clinics (CBOCs).

In terms of the system composition, each EHRM Audiology end user device (EUD) or clinical workstation has two Cerner-provided applications installed on top of the VA standard Windows 10 image with VA security & system monitoring tools suite: AudBase User Interface (UI) application and Citrix Receiver. Other VHA-procured audiology applications are HIMSA Noah 4, Audioscan Noah Module, Cochlear Bone Anchored Solution, Cochlear Custom Sound suite, GN OTO suite & Granson-Stadler GSI suite, Interacoustics AS suite, Oticon AS Genie, Phonak Target, Sivanto Signal Fitting package, Starkey Hearing Technologies Inspire, Unitron TrueFit. AudBase UI collects and aggregates hearing test data and from the audiology applications then converts them into comprehensive reports that can be ingested by the AudBase Server in the Joint EHR/Federal Enclave. Citrix Receiver provides audiologists access to patient records in the Joint EHR database via the PowerChart application. Role-based access control rules would define the number of clinical records each audiologist/user can access to, from a handful to millions. None of the afore-mentioned audiology applications would retain or store patient personally identifiable information (PII) and/or protected health information (PHI).

No change to business processes or technology of the EHRM Audiology Workstations system is expected once this Privacy Impact Assessment is completed. No cloud technology is used within the boundary of the system.

The authority to operate the system is stated in Title 38, United States Code (U.S.C), § 501(b) and § 304. In compliance with the Federal Information Security Modernization Act (FISMA) of 2014, the system must receive a security authorization to operate, or an ATO, given by a senior VA authority official or an AO. In this management decision, acting on behalf of the VA, the AO would explicitly accept the risk to agency operations including mission, functions, image, or reputation, agency assets, individuals, etc. based on the implementation of an agreed-upon set of security and privacy controls defined by Directive 6500, VA Cybersecurity Program. The authority for the system to collect, use, and disseminate information about individuals that is maintained in systems of records by federal agencies, in accordance with the code of fair information practices established by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, is stated in System of Record Notification (SORN) 24VA10A7, Patient Medical Records-VA, the same SORN used by the Joint EHR system. No amendment or revision of the existing SORN is needed as part of EHRM Audiology Workstations deployment.

Section 1. Characterization of the Information

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

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

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

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

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

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
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

Electronic Data Interchange Personal Identifier (EDIPI), patient clinical encounter data such as audiology, modality, hearing test data, diagnosis procedures and results

PII Mapping of Components

The EHRM Audiology Workstations system consists of zero (0) key component (database). Each component has been to determine if any elements of that component collect PII. The type of PII collected by EHRM Audiology Workstations system and the reasons for the collection of the PII (if any) are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.10 in the PTA should be used to answer this question.

PII Mapped to Components

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

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

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

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

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

The sources of the PII/PHI processed by the audio-aid modules in the Audiology Workstations system is the Joint EHR system and the AudBase server resided in the Federal Enclave, external to VA information system boundary. EHRM Audiology Workstations system does not collect information directly from individual patients.

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.

EHRM Audiology workstation does not collect information directly from individual patients. Instead, they receive patient information via electronic transmission from the Joint EHR system.

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

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

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

EHRM Audiology Workstations is a user interfacing system. By design, it does not check information accuracy. Instead, the AudBase server located in the Federal Enclave would run accuracy check then communicate with the AudBase UI installed in the Audiology workstation.

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

The authority to operate the system is stated in Title 38, United States Code, Sections 501(b) and 304. The authority for the system to collect, use, and disseminate information about individuals that is maintained in systems of records by federal agencies, in accordance with the code of fair information practices established by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, is stated in SORN 24VA10A7, Patient Medical Records-VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk: There's a risk that an audio-aid module may collect more PII than it was supposed to.

Mitigation: Each of the twelve (12) audiology applications being installed in the EHRM Audiology Workstations system has been reviewed and approved by the VA Technical Review Model (TRM) group to ensure VA/VHA technical, functional, patient safety, and cybersecurity standards/requirements are met. Only data elements needed for audiology purpose are collected and processed by the applications.

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.

- Patient (Full) Name is used to identify the correct patient for clinical care purpose
- Date of birth is used to identify the correct patient
- EDIPI is used to identify and ensure the correct patient; EDIPI of VA employee is used to verify and authenticate system/device access

- Clinical encounter data such as audiology, modality, hearing test data, diagnosis procedures and results to assist the care provider in diagnosis and monitoring patient care progress.

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

No tool is used by EHRM Audiology Workstations to analyze or produce data.

2.3 How is the information in the system secured?

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

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

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

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

Transmission Control Protocol/Internet Protocol (TCP/IP) Hypertext Transfer Protocol Secure (HTTPS) Transport Layer Security (TLS) 1.2, is used to protect data in transit.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>Example: Describe if training for users of the project</u>

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.

In order to access the EHRM Audiology Workstations system, a user must first have granted access to the Joint EHR system, based on the Need-to-Know principle. As part of FISMA compliance, relevant access controls, identification and authentication controls, and personnel security controls have been designed and implemented for the system.

Section 3. Retention of Information

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

3.1 What information is retained?

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

No record with the collected data elements as identified in question 1.1. is retained by Audiology Workstations. As a user interfacing system, Audiology Workstations would return information back to the AudBase server in the Federal Enclave.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

No record with the collected data elements as identified in question 1.1. is retained by Audiology Workstations. As a user interfacing system, Audiology Workstations would return information back to the AudBase server in the Federal Enclave.

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.

No record with the collected data elements as identified in question 1.1. is retained by Audiology Workstations. As a user interfacing system, Audiology Workstations would return information back to the AudBase server. AudBase server follows instructions provided by VHA RCS 10-1, item number 1004.1, Tracking and Control Records, page 14
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

Since EHRM Audiology Workstations is a user interface system and does not store/retain patient records, VA Office of Information and Technology (OI&T) electronic media sanitization procedures will be used at the end of the system life cycle.

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

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

The system does not use data for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Privacy Risk: A risk may arise when a live session is left open inactively on the workstation monitor screen longer than it should be and exposes patient records to unauthorized viewers.

Mitigation: Session time-out access control has been designed and will be implemented to close out inactive sessions, after a pre-defined period of time in accordance with VA Directive 6500.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Privacy Risk: Patient care data displayed on the audiology workstation monitor and may be viewed by un-authorized people.

Mitigation: To ensure PII/PHI displayed for and viewed by only the authorized care provide, a combination of security controls such as verify user's assigned profile from Active Directory Role Management Server, security awareness and training, access control to automatically terminate inactive sessions, etc. have been implemented and validated.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Defense Health Agency (DHA)/Federal Enclave/Joint EHR/AudBase	Medical care treatment	Name, date of birth, EDIPI, clinical encounter data such as audiology, modality, hearing test data, diagnosis procedures and results	Memorandum of Understanding (MOU) between Department of Defense (DoD) and VA for Sharing Personal Information, March 2014	Transport Layer Security (TLS), Citrix Independent Computing Architecture (ICA)

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

Privacy Risk: VA patient records stored in the Joint EHR system/Federal Enclave, a cybersecurity boundary authorized and managed by DOD/DHA, an external Federal agency, may be exposed to certain privacy risks such as unauthorized access or being used for purposes other than the stated purpose and use of the original collection.

Mitigation: Beside the afore-mentioned MOU jointly signed between DoD and VA in March 2014, the two agencies have entered in other inter-agency cybersecurity agreements such as the MOU for Authority to Operate (ATO) Reciprocity dated January 24, 2018, the MOU for Implementation of the Medical Community of Interest (Med-COI) Network dated November 6, 2019, the Interconnection Security Agreement between DHA and VA OI&T concerning the Enclave supporting the EHRM Programs dated April 22, 2020. Accordingly, in compliance with the FISMA Reform of 2014, all VA EHRM systems resided in the Federal Enclave are required to obtain an ATO authorized by the DHA AO and then by the VA AO following the reciprocity process. Access and audit controls have been selected and implemented for these EHRM systems. They are parts of the 18 security control families recommended by the National Institute of Technology and Standards (NIST) Special Publication (SP) 800-53 Revision 4 and in compliance with VA Handbook 6500, Risk Management Framework for VA Information Systems – VA Information Security Program dated Feb 24, 2021.

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.

The EHRM Audiology Workstations system does not collect PII/PHI directly from individual patients. The system receives or "collect" information via electronic transmission from the Joint EHR system and AudBase server located in the Federal Enclave. Reference SORN 24VA10A7, Patient Medical Records-VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx), VHA Notice of Privacy Practices (NOPP) (http://www.va.gov/health/) which is provided to a patient in person for services and can be mailed to eligible Veterans every 3 years by the VHA.

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

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

The EHRM Audiology Workstations system does not collect PII/PHI directly from individual patients. Instead, it receives or "collects" information via electronic transmission from the Joint EHR system and AudBase server located in the Federal Enclave. Individuals do have the opportunity and right to decline to provide information as having described in SORN 24VA10A7, Patient Medical Records-VA, VHA Handbook 1605.04, Notice of Privacy Practices (NOPP). The latest publication of the VHA NOPP can be found at this link http://www.va.gov/health/. A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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

The EHRM Audiology Workstations system does not collect PII/PHI directly from individual patients. Instead, it receives or "collects" information via electronic transmission from the Joint EHR system and AudBase server located in the Federal Enclave. Individuals do have the right to consent to particular uses of the information as having described in SORN 24VA10A7, Patient Medical Records-VA, VHA Handbook 1605.04, Notice of Privacy Practices (NOPP). The latest publication of the VHA NOPP can be found at this link http://www.va.gov/health/. A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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

Privacy Risk: An individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the VA prior to providing the information.

Mitigation: This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans present for service. New NOPPs are mailed to the patients/Veterans every 3 years and periodic monitoring is performed to check that the acknowledgment form signed by patients have been scanned into electronic records. Additional mitigation is provided by making the System of Record Notices (SORNs) and NOPP available for review online (https://www.oprm.va.gov/privacy/systems_of_records.aspx) (http://www.va.gov/health/)

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.

EHRM audiology workstation does not collect PII/PHI directly from individual patients. Instead, they receive or "collect" information by means of interfacing with the Joint EHR system. Reference SORN 24VA10A7, Patient Medical Records-VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx), VHA Notice of Privacy Practice (http://www.va.gov/health/), VHA Directive 1605.01, Privacy and Release of Information, VA Handbook 6300.3 -Procedures for Implementing the Freedom of Information Act.

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 https://www.va.gov/find-forms/about-form-10-5345a

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. More information about myHealthevet is available at https://www.myhealth.va.gov/index.html

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.

Individual patients have the right to request an amendment (correction) to their health information in VHA records if they believe it is incomplete, inaccurate, untimely, or unrelated to your care. The individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient's

information or health records. Reference "Right to Request Amendment of Health Information" under VHA Notice of Privacy Practices (NOPP) (https://www.va.gov/health/).

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.

According to section "Right to Request Amendment of Health Information" under VHA NOPP, the individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient's information or health records.

For the latest version of the VA Privacy Practices, check the VHA Privacy Office web portal https://www.va.gov/health/ then click on VA Privacy Practices under the "Resources" section to the right of the page.

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.

If an individual/patient's request for amendment is denied, they will be notified of the decision in writing and given information about their right to appeal the decision. In response, the individual may do any of the following:

- File an appeal.
- File a "Statement of Disagreement" which will be included in your health record
- Ask that your initial request for amendment accompany all future disclosures of the disputed
- health information

Reference "Right to Request Amendment of Health Information" under VHA Notice of Privacy Practices (NOPP) (https://www.va.gov/health/).

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.

Privacy Risk: Individuals whose records contain incorrect or out-of-date information may be exposed to the risk of not receiving prescription medications, notification of appointments, or test results timely. Certain incorrect information in a patient medical record could result in improper diagnosis and treatments.

Mitigation: Various accuracy checks are designed and implemented in different workflows of the Joint EHR system. VHA built-in procedure requires staff verify information in patient medical records and correct information identified as incorrect during each patient's medical appointments. Staff are informed of the importance of maintaining compliance with VA Request of Information policies and procedures and the importance of remaining alert to information correction requests. Individual patients have the right to request an amendment (correction) to their health information in VHA records if they believe it is incomplete, inaccurate, untimely, or unrelated to your care. The individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient's information or health records. Reference "Right to Request Amendment of Health Information" under VHA Notice of Privacy Practices (NOPP) (https://www.va.gov/health/).

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.

In order to access the EHRM Audiology Workstations, an audiologist must first be granted access to the Joint EHR system.

Access to a certain role in the Joint EHR system is determined by the user's manager/supervisor (accountable individual) and the Using Service for the purposes of performing official assigned duties. Access to an EHRM system is restricted to VA employees and contractors who must complete both the VA Privacy and Information Security Awareness and Rules of Behavior (ROB) course and the VHA Privacy and HIPAA Focused Training course. Specified access is granted based on the employee/contractor functional category. Role based training is required for individuals with significant information security responsibilities.

An audiologist uses his/her VA Personal Identity Verification (PIV) card and Personal Identification Number (PIN) to authenticate into his/her Audiology workstation or EUD. The authorized clinician invokes the Citrix Receiver and launches a Citrix session and passes his/her authenticated credential to Citrix NetScaler. Citrix secure Independent Computing Architecture (ICA) connection provides XenDesktop via Citrix virtual desktop infrastructure (VDI) using user's assigned profile from Active Directory (AD) Role Management Server to the Joint EHR System Citrix Portal to access user-facing published clinical applications.

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.

No VA contractor personnel will be granted access to the EHRM Audiology Workstations system under a defined Joint EHR system role. A limited number of contractor personnel, however, may be periodically granted admin or system access right to perform system maintenance and technical troubleshoot upon request by the system owner.

All contractor personnel must comply with VA cybersecurity and data safeguarding requirements, including contractor confidentiality agreement, Business Associate Agreement, and Non-Disclosure Agreement signed between Cerner Corporation/Cerner Government Services and the EHRM IO.

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.

Contractor personnel with access to VA information or information systems must read and acknowledge their receipt and acceptance of the VA Privacy and Information Security Awareness and ROB course or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

If Yes, provide:

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

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

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

In Process. EHRM IO is working on the ATO package for EHRM Audiology Workstations and expects to submit a complete package to the VA AO for review and approval in quarter 3, FY22. In

compliance with the FISMA of 2014 and Federal Information Processing Standards Publication 199, the system has been categorized at MODERATE impact level. A set of NIST SP 800-53 Rev 4 security and privacy controls has been selected to implement for the system, commensurate with the Moderate impact level and in compliance with VA Handbook 6500 – RMF for VA Information Systems – VA Information Security Program. Implementation and compliance status of each security/privacy control applicable to the system is registered in Enterprise Mission Assurance Support Service (eMASS), a web-based Government off-the-shelf (GOTS) service for Risk Management Framework (RMF) Assessment and Authorization activities with capability to support continuous monitoring cybersecurity compliance model. Multiple draft versions of the System Security Plan (SP), one of the five RMF required artifacts, can be quickly generated from eMASS to provide a snapshot of the Work-in-Process ATO package with listing of assigned security and privacy controls, their implementation status, personnel and justification required for validation. An official and final SP version with signature of the system owner, however, is not needed and won't be generated until ATO package artifacts are assembled and submitted to the VA AO as part of eMASS RMF Workflows.

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).

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

EHRM Audiology Workstations system does not use cloud technology.

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)

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 they provided in this Privacy Impact Assessment is true and accurate.

Gina A Siefert 273290

Digitally signed by Gina A Siefert 273290
Date: 2022.06.29 07:53:20 -05'00'

Privacy Officer, Gina Siefert

JERAMY A. DRAKE 505947

Digitally signed by JERAMY A. DRAKE 505947
Date: 2022.06.28 10:26:27 -07'00'

Information System Security Officer, Jeramy Drake

Michael J. Hartzell 3487012

Digitally signed by Michael J. Hartzell 3487012
Date: 2022.06.28 14:23:32 -04'00'

Information System Owner, Michael Hartzell

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).

For the latest version of the VA Privacy Practices, check the VHA Privacy Office web portal https://www.va.gov/health/ then click on VA Privacy Practices under the "Resources" section to the right of the page.