



Privacy Impact Assessment for the VA IT System called:

Enterprise Wide Speech Recognition (EWSR) Dragon Medical One (DMO)

Enterprise Program Management Office; Transition, Release and Support (TRS) division

Date PIA submitted for review:

December 4, 2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian D. Loftus	Christian.Loftus@va.gov	(859) 281-2470
Information System Security Officer (ISSO)	Amine Messaudi	Amine.Messaoudi@va.gov	(202) 815-9345
Information System Owner	Julie Schuck	Julie.Schuck@va.gov	(515) 778-3535

Abstract

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

Dragon Medical One (DMO) Software as a Service (SaaS) allows the VA to harness emerging technology to realize its goal of transformation into a 21st century care delivery organization that can best support America’s Veterans. Enterprise-Wide cloud-based speech is a leap forward in the human-machine interface and is a key component in healthcare today.

Overview

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

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

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

The Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO) has a requirement for a Brand Name or Equal to Dragon Medical One (DMO) Software-as-a-Service (SaaS) solution for Medical-Specific Enterprise-wide Front-End Speech Recognition System for non-Radiology applications. Most clinical documentation in the Veterans Health Administration (VHA) resides in the Computerized Patient Record System (CPRS), the VA's highly regarded Electronic Health Record (EHR).

VHA previously used Nuance's Dragon Medical Network Edition (DMNE) as their primary speech recognition software used by VA non-radiologists. DMNE was hosted in VA datacenters and no longer met the stricter mandated security requirements such as two factor authentication (2FA). In an effort to meet improved security guidelines and the push to use cloud-based computing, OI&T contracted to use Nuance's Dragon Medical One (DMO) SaaS solution for direct medical transcription into patient records. This will result in improving productivity and user satisfaction of clinicians, reduce cost of transcription, improve accuracy and quality of medical documentation, and ultimately enhance patient-centered care.

Nuance's proposed Dragon Medical One (DMO) SaaS solution will allow the VA to harness emerging technology to realize its goals with an industry-leading solution for real-time, cloud-based medical speech recognition. This solution will make use of a FedRAMP authorized portion of the Microsoft Azure Cloud.

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:

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

Date of encounter

PII Mapping of Components

Enterprise Wide Speech Recognition (EWSR) Dragon Medical One (DMO) SaaS solution consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise Wide Speech Recognition (EWSR) Dragon Medical One (DMO) SaaS solution and the reasons for the collection of the PII are in the table below.

- Electronic Health Record (EHR)
- VistA
- Computerized Patient Record System

PII Mapped to Components

PII Mapped to Components

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

Electronic Health Record (EHR)	Yes	Yes	Name, Date of Birth, Date of encounter, Health data	Speech to text conversion for EHR	National Institute of Standards and Technology (NIST)
Computerized Patient Record System	Yes	Yes	Name, Date of Birth, Date of encounter, Health data	Speech to text conversion for EHR	National Institute of Standards and Technology (NIST)
Vista	Yes	Yes	Name, Date of Birth, Date of encounter, Health data	Speech to text conversion for EHR	National Institute of Standards and Technology (NIST)

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.

Clinicians dictate patient data, medications, tests, diagnosis, etc. into a microphone connected to their computer or into their government furnished cell phone with the PowerMic Mobile (PMM) application installed. This voice data is analyzed by the Dragon Medical One (DMO) servers, converted into text, and entered the selected CPRS field.

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.

Dragon Medical One (DMO) does not use any identifiable PHI and only stores snippets of actual dictation. The audio snippets are non-contiguous. Audio Snippets are associated with the voice profile of the user. Dragon does not have the capability to search the database by identifiable PHI or by patient.

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

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

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

Name – identification

DOB – identification

Medical Record Number – updating CPRS with clinician's dictation

Date of encounter – updating CPRS with clinician's dictation

Current medications – updating CPRS with clinician's dictation

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information is checked in real time by the clinician as the text is entered into CPRS. PII and PHI data is not used/collected/stored in the DMO system. PII and PHI is only used to update CPRS.

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

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

This question is related to privacy control AP-1, Authority to Collect

5 USC 552a, 45 CFR § 164.506, 38 USC 5701(b)(3), SOR 24VA10A7
(https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf) Patient Medical Record–Routine Use #29.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is PII/PHI data shared with the system. The system translates audio directly into text into CPRS. There is a risk of errors from dictation to text and incorrect information being stored in CPRS. There is a risk anytime PII/PHI is shared.

Mitigation: No PII/PHI is stored in the DMO system. The only data stored is audio snippets of what is explicitly said by the clinician. This limits the risk of accessing PII/PHI. The clinician is dictating and viewing the text that populates in real time so any errors in voice/speech recognition can be seen and corrected right away. Providers can use voice commands to correct text or they can type corrections directly.

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.

There is no PII or PHI stored in the system. The business purpose is for clinicians to be able to use dictation to update CPRS. The information shared is name, date of birth, medical record, and date of encounter. This information is required for the identification and to update CPRS.

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

Speech recognition software to analyze audio from microphone connected to their computer or into their government-furnished cell phone with the PowerMic Mobile (PMM) and convert dictation to text. The mic is not proprietary, and any mic would work with this software. Then the text is entered to update CPRS.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The PII and PHI is not stored or accessed through DMO so this is not applicable.

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 PII or PHI is retained. DMO only stores audio snippets of what the provider explicitly dictates. These audio snippets are non-contiguous and not associated with an individual. The audio snippets are associated with a voice profile of the provider.

3.2 How long is information retained?

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

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

No PHI or PII is stored or retained by DMO. The only data stored is audio snippets of what the provider explicitly dictates. This data is kept indefinitely.

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

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

Yes, RCS 10-1, 6000.2 Electronic Health Record. Temporary. Destroy/delete 75 years after the last episode of patient care. N1-15-02-3, item 3

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

No SPI stored so this is N/A.

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

N/A

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk of access to the audio snippets. These are stored for a longer period of time and therefore have a greater risk of being unintentionally breached.

Mitigation: The audio snippets are non-contiguous so it would be difficult to discern any clear information or meaning from the clips if they were unintentionally breached. There is no other data stored in DMO system. Dragon Medical one is accessible only to authorized users and deployed on in dedicated subnets on the Project Hosts Federal Private Cloud. The subnets and services are all protected using Azure Network Security Groups at the subnet and NIC level or similar Azure access controls for the PaaS services configured according to the principle of least privilege in a deny all, allow by exception mannerism to and from specific IP addresses on specifically approved ports using approved protocols. Additionally, all data is encrypted at rest using Azure storage Service encryption. End user customers authenticate first to their Agency Federation Services, then to the NU-DMO application via SSOi Federated authentication. The Nuance DMO solution distributes application traffic to two Azure regions through Azure Traffic Manager profiles, which effectively direct clients to the Azure region which offers the lowest network latency for their specific location, delivering the specific DNS record for those region's Azure endpoints. Traffic Manager is also leveraged for the application Contingency Plan by automatically directing users to the alternative region DMO deployment when there is a region failure, both simulated and live. Once traffic is directed by the traffic manager it then traverses the web application proxy servers in the FPC DMZ subnet to Nuance HA Proxy servers. The WAPs provide application level firewall functionality including port blocking, IP filtering, TLS encryption, intrusion detection and alerting. Pre-authentication is required and protects the backend application by terminating the external session and starting another one with the backend application which eliminates layer 2 and 3 attacks. The WAPs also decrypt traffic prior to analysis in order to filter html calls and drop mal-formed html packets. All servers are configured according to the deny all allow by exception policy and access is controlled by Azure Network Security groups and all external communications are monitored using HIPS software .

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system	Describe the method of transmittal
Veteran’s Health Administration	Transcription- Transcriptions from clinicians entering information into the DMO application which functions by taking a clinician’s speech and dictating it back to text inside of the DMO client on the clinicians workstation. This text is then reviewed by the clinician and accepted ensuring its accuracy. This transcription could include anything the doctor chooses to have converted within the application including information about patients and their health conditions.	Name, DOB, Current medications, Date of Encounter, Medical Record #	https over port 443

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguard are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, ad required reporting of suspicious activity

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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 Notice of Privacy Practices (see attached). 24VA10A7/85 FR 62406 Patient Medical Record in the Federal Register.

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

There is no explicit consent between the patient and DMO. However, there is no PII/PHI stored in DMO. DMO is used to update the CPRS Medical Record and the only information is what the doctor explicitly dictates. Any information shared from patient to doctor is privileged communication.

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

There is no explicit consent between the patient and DMO. However, there is no PII/PHI stored in DMO. DMO is used to updated CPRS Medical Record and the only information is what the doctor explicitly dictates. Any information shared from patient to doctor is privileged communication.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is risk that an individual may not receive notice that their information is being converted from audio to text by DMO through clinician dictation.

Mitigation: The individual is notified of their information being stored as their medical record in CPRS. Only the non-contiguous audio snippets are being stored in DMO and DMO is only the vessel to convert this information from speech to text. The individual sharing of information with the clinician is privileged and the clinicians complete HIPAA and privacy training.

Section 7. Access, Redress, and Correction

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

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

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

http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

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

The individual is notified of their information being stored as their medical record in CPRS. Only the non-contiguous audio snippets are being stored in DMO and DMO is only the vessel to convert this information from speech to text. The individual sharing of information with the clinician is privileged and the clinicians complete HIPAA and privacy training.

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.

The individual is notified of their information being stored as their medical record in CPRS. Only the non-contiguous audio snippets are being stored in DMO and DMO is only the vessel to convert this information from speech to text. The individual sharing of information with the clinician is privileged and the clinicians complete HIPAA and privacy training.

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.

If a patient were to become aware of an error in their CPRS medical record file they would work with their doctor directly to correct any incorrect information in their chart. The patient will not interact through DMO in any capacity. Doctors are trained using VA's Talent Management System (TMS) on how to use DMO including how to correct errors

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 ensure data accuracy.

N/A See Above, 7.3

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: *Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

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

Principle of Individual Participation: *Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that DMO could have errors in converting audio to text.

Mitigation: Clinicians are viewing the text in CPRS in real time. The ability to correct errors is much like typing in that clinician can delete, add additional text, or highlight and dictate over incorrect information. These corrections can be made in real time by using DMO or by manually typing in CPRS without DMO.

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.

Only VA Clinicians will have access to the PII fields. No third-party organization will have access to PII. All response data resides in the DMO Service within the Project Hosts Federal Private Cloud deployed in turn on Azure Government (environment is specific only for Federal customers), and data is encrypted at rest using Azure Service Storage Encryption. Nuance requires the platform to be FedRAMP authorized.

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

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

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

Since this is a SaaS solution hosted external to the VA network, the vendor team will design and maintain the system. As part of VA onboarding, the contractor will sign an NDA. Contractors will not have access to PII/PHI as PII/PHI are not stored in the system.

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

Training required per the contract is:

- A. VA Privacy and Information Security Awareness and Rules of Behavior
- B. Signed Contractor Rules of Behavior
- C. VA HIPAA certificate

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.

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

If Yes, provide:

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

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

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

No, an A&A has not been completed for this system. Project Host is working with Nuance to complete the FedRamp certification. The FIPS 199 classification is low as per Data Security Categorization and System Security Categorization.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Privacy Officer, Christian D. Loftus

Information Systems Security Officer, Amine Messaudi

System Owner, Julie Schuck

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).