Privacy Impact Assessment for the VA IT System called:

Zeto EEG

Epilepsy Center of Excellence VHA; Central Virginia Healthcare System (CVHCS), Richmond, VA

Date PIA submitted for review:

Jan 18, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Marie Montamabadou*	*vharicprivacyofficer@va.gov* *Marie.Montamabadou@va.gov*	*804-675-5265*
Information System Security Officer (ISSO)	*Yvonne I. Goudy-Bermudez*	*vharicisosupport@va.gov* *Yvonne.Goudy-Bermudez@va.gov*	*804-675-5000 x1017*
Information System Owner	*Fred Tolley*	*fred.tolley@va.gov*	*202-461-9005*

Abstract

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

The Zeto EEG system is a cloud-based platform that communicates and receives neurobiological data in the form of electroencephalogram (EEG) or "electrical brain wave activity" on Veterans who are evaluated for epileptic seizures. This system allows acquisition of EEG data in versatile ways by non-neurologist or technician staff in areas or settings where such personnel are not available. The IT system involves website control of the EEG headset for data acquisition and website review of data by specialized personnel who can then report and guide management to local staff.

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?*

The WR19 digital electroencephalograph system measures electrical potential caused by cerebral activity on the scalp. WR19 is a full montage EEG and contains 19 electrodes *located according to the International 10-20 EEG system. These electrodes produce 19 channels of clinical quality EEG data.*

The WR19 System is intended for prescription use in the health care facility or clinical research environment to acquire, transmit, display and store primarily EEG and optionally auxiliary signals for adults and children, not including newborns.

The WR19 System requires operation by a healthcare professional familiar with EEG. The WR19 System acquires, transmits, displays and stores electroencephalogram (EEG), and optionally electrocardiogram (ECG), accelerometer, photic sensor, external trigger signals and video.

WR19 records neurobiological data in the form of electroencephalogram (EEG) or "electrical brain wave activity" on Veterans who are evaluated for epileptic seizures. This system allows acquisition of EEG data in versatile ways by non-neurologist or technician staff in areas or settings where such personnel are not available.

Zeto WR19 EEG headset comes with a full software infrastructure for controlling the headset, managing studies, interpreting recordings and managing patient data. This system and its components are called the Zeto Cloud Platform (ZCP).

ZCP (Zeto Cloud Platform) acquires, stores, retrieves studies of biopotential signals such as EEG and ECG signals. These studies may contain PHI in electronic format, such as patient name, and full face video.

Zeto WR19 headset is a wireless EEG headset with direct connection to ZCP. Alternatively, WR19 headset connects to a receiver box (Zeto Interface Box - ZIB) connected to a Windows 10 based computer provided by the Healthcare provider (Customer) and uses the existing wired or wireless connection of that computer. The headset does not handle PHI.

ZHI (Zeto Hosted Interface) is a client application. Users of ZCP can control headset(s), start studies, and interpret recordings using the ZHI client. Users may enter PHI and access it using this application.

The Zeto Cloud Platform is owned, developed and operated by Zeto, Inc. Since ZCP is a cloud based platform, there is very little IT infrastructure needed at the VA facilities.

Operators enter patient PHI such as name, date of birth into the system in order to identify EEG studies. Operators may use the video recording functionality of the platform to record facial and limb movements of the patient during an EEG study. This information carries diagnostic clinical value. Patient PHI is stored for the convenience of the operators and physicians interpreting the EEG studies and completing a diagnosis of the patient.

The system comes with a complete authentication and authorization scheme. Name, email address, and optionally phone number of the operators, physicians and other users (PII) are stored in the system. Name is stored for audit logging purposes; email is stored for the *purpose of secondary authentication during lost password reset functionality. Phone number is required in case text message-based MFA authentication is enabled.*

There is no built-in data transmission or sharing of PHI or PII with any other system (neither Zeto nor VA systems). PHI or PII is solely available for the operators of the system on the ZHI client application, and via a separately enabled API access. Operators are able to enter, edit PHI and download EEG studies and video recordings which may contain PHI, and are expected to be HIPAA compliant. All Zeto personnel and the system are HIPAA compliant.

- *The Zeto Cloud Platform is a distributed cloud system working in multiple physical regions in order to provide low latency access to everywhere in the country. All regions use the same physical and cybersecurity controls and run the same release of the software components. Since the Zeto Cloud Platform is a cloud-based system, it is available for all VA sites.*

ZCP platform is running on AWS cloud, and operated by Zeto Inc.

Completion of this PIA will not result in any changes in the system. The system is not SORN listed at the time of completing this form.

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)

[X] email address of the operator (user)
[X] handedness (dominant hand) (patient)

The list above shows a comprehensive overview of what ZCP platform is able to store. Please note that all information is optional.

For operators of the system, an IP address is collected for audit logging purposes, an email address for identification, and a personal phone number is required for text message-based MFA authentication.

PII Mapping of Components

Zeto EEG consists of 3 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Zeto EEG and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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
global login	No	Yes	email address, phone number	user login authentication	encryption at transit, encryption at rest, access authorization
zcp	Yes	Yes	name, DOB, SSN, Medical record number, gender, handedness, medication, medical records full face video	searching EEG studies by patient data, completing diagnostic EEG reports with patient data clinically relevant movements of the patient during EEG study	encryption at transit, encryption at rest, access authorization

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.

User data: *name of the operators, email address, optional phone number provided by VA is entered into the system initially by Zeto personnel. Further on, VA administrative personnel manage users.*

Patient data: *the operator starting an EEG study enters patient data such as name, date of birth manually. This data is provided by the patient or based on an external patient management system.*

Full face video: *during the EEG study, the system is able to record video streams. The operator controls whether the study runs with or without a camera.*

Existing medical records: *the operator may upload existing medical records to the system in order to provide complete information for the diagnosis. These files are coming from external sources, Zeto Cloud Platform works solely as a file storage mechanism.*

EEG reports: *a physician interpreting an EEG study may use the built-in report generator in order to produce a final diagnosis and a report. The report can be downloaded from the system in PDF, and docx (Word) format, or can be copied into an external EHR system via clipboard.*

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 technologies 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.

User data: *initial user data is collected by the Zeto Customer Success team in advance prior to deploying the system using an online form.*

Patient data: *the operator enters patient data manually - source of the data is not relevant.*

Full face video: *camera records the video stream.*

Existing medical records: *the operator uploads electronic files, such as PDF, docx, or image files.*

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.

Zeto Cloud Platform has no connections to external systems, hence no automatic check for accuracy is in place.

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.

"The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. 31 CFR § 1.32 - Use and disclosure of social security"

This question is related to privacy control AP-1, Authority to Collect
Zeto EEG is a facility level entity that operates under the authority of Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:
• Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
• Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.
• Privacy Act of 1974, 5 U.S.C. 552a

• Federal Information Processing Standards (FIPS) 140-2, approved encryption algorithms and products
• Federal Information Processing Standards Publication (FIPS PUB) 199, Standards for Security Categorization of Federal Information and Information Systems
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 60, Guide for Mapping Types of Information and Information Systems to Security Categories.
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, Recommended Security Controls for Federal Information Systems
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Guidelines for Media Sanitization
• Zeto EEG VA Health Care System local MCP 00PO.01, Privacy Policy.
• Trade Secrets Act (18 U.S. Code 1905)
• Unauthorized Access Act (18 U.S. Code 2701 and 2710)
• VA Directive 6371, Destruction of Temporary Paper Records
• VA Directive 6600, Responsibility of Employees and Others Supporting VA in Protecting Personally Identifiable Information (PII)
• VA Directive and Handbook 6500, Information Security Program
• VA Directive and Handbook 0710, Personnel Suitability and Security Program
Version Date: May 20,
2021 Page 14 of 45
Legal Authority Table
Site Type: VBA/VHA/NCA
or Program Office
Legal Authority
VHA • Veterans Health Administration – Organization and Functions,
Title 38, U.S.C., Chapter 73, § 7301(a)
• Health Insurance Portability and Accountability Act of 1996
(HIPAA)
• Privacy Act of 1974
• Freedom of Information Act (FOIA) 5 USC 552
• VHA Directive 1605.01 Privacy & Release of Information
• VA Directive 6500 Managing Information Security Risk: VA
Information Security Program

SORN:

24VA10A7/ 85 FR 62406	Patient Medical Records-VA
121VA10A7/ 83 FR 6094	National Patient Databases-VA

https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

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.

Zeto Cloud Platform is not connected to external data sources, automatic integrity checks are not implemented.

Follow the format below when entering your risk assessment:

Privacy Risk: Zeto EEG sensitive personal information – including social security numbers, names, dates of birth and protected health information – on veterans, members of the public, & VA employees and contractors. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: Zeto EEG as well as the Richmond Veterans Health Care System deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. The security measures include access control, configuration Version Date: May 20, 2021 Page 15 of 45 management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

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.

User data: *collecting name is required for audit logging, email for password change authentication, optional phone number is for MFA based authentication.*

Patient data: *all data elements are optional, these helps searching and identifying EEG studies later on, and grouping recurring EEG studies on the same patient, and simplifying generation of the EEG reports. Birth date allows calculation of patient age. Age and handedness are clinically relevant attributes when interpreting an EEG and completing a diagnosis.*

Full face video: *Video during routine EEG activation procedures is clinically relevant when interpreting an EEG and completing a diagnosis.*

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

Report generator: *With the help of the system, a physician interpreting the EEG can complete an EEG report explaining the status of the patient and the diagnosis. This* *report is stored attached to the patient record in the system, and available for downloading and importing to external Electronic Health Record (EHR) systems.*

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?

If data in transit and at rest is encrypted

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

Collecting and retaining SSN is optional. There is no additional protection in place at this time. SSN is encrypted.

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

Zeto Cloud Platform is designed and audited to HIPAA/HITRUST.
Encryption of PII/PHI in transit and at rest is implemented as per NIST SP800-53.
User authentication and authorization are implemented as per NIST SP800-53.
Password policies and password complexity checks are implemented as per NIST SP800-53.
Our cybersecurity objective is to start the FedRAMP certification process in Q1 2022, which ensures even more comprehensive PII/PHI safeguards.

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

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 covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.</u>

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

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

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

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

Zeto personnel: *Zeto personnel are HIPAA trained by the Privacy Officer. Training logs are maintained. Each individual is aware of a list of our HIPAA policies, including PHI policy, and disciplinary actions in case of unauthorized access or misuse of PHI. Violating the policy may result in an adverse employment action up to and including termination.*

Use of information, limitation of use: User data: *collecting name is required for audit logging, email for password change authentication, optional phone number is for MFA based authentication.*

Use of information, limitation of use: Patient data: *all data elements are optional, these help searching and identifying EEG studies later on, and grouping recurring EEG studies on the same patient, and simplifying generation of the EEG reports. Birth date allows calculation of patient age. Age and handedness are clinically relevant attributes when interpreting an EEG and completing a diagnosis.*

Use of information, limitation of use: Full face video: *Video during routine EEG activation procedures is clinically relevant when interpreting an EEG and completing a diagnosis.*

Section 3. Retention of Information

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

3.1 What information is retained?

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

- *Name*
- *Social Security Number*
- *Date of Birth*

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.

Zeto Cloud Platform retains all data in the cloud, as much as the data storage purchased. Data is disposed solely at VA's request. Physical destruction of data storage media is as per NIST 800-88 Guidelines for Media Sanitization.

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, Records Control Schedule 10-1 (va.gov)

Records Control Schedule 005-1

Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B.

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

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500, Electronic Media Sanitization (November 3, 2008),

https://www.va.gov/vapubs

. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500. Digital media is shredded or sent out for destruction per VA Handbook 6500.

Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

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

There is no test/training data in the database when deploying the system to VA.

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:

Storing excessive amounts of PII affects the impact of a potential data leak/breach or unauthorized access.

Mitigation:

Zeto Cloud Platform has means for limiting the number of PII records (e.g. store up to 500 patient records) in order to minimize the risk.

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 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:
<u>Privacy Risk:</u>
N/A - Zeto is not aware of any internal sharing between internal VA organizations.

<u>Mitigation:</u>
N/A - Zeto is not aware of any internal sharing between internal VA organizations.

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***
Zeto EEG	To Identify and troubleshoot problems in the systems.	Name, Date of Birth	MOA	Secure Wed-Portal

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:
If data including PHI is physically stored on AWS (encrypted in the move and at rest) was to be hacked.

Mitigation:

Zeto has a BAA with AWS covering HIPAA requirements

Privacy Risk:
If downloading data with the API functionality (this enables downloading EEG studies and video which is PHI, used by 3rd party integrations) was compromised.

Mitigation:
VA does not require this functionality, so this won't be enabled.

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.

Electroencephalogram (EEG) acquired by the Neurology service via a Zeto device follows the privacy practices laid out by VHA Directive 1605.01 https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false

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

Individuals retain the right to decline to provide information. This would prohibit documentation of test findings to the patient's medical record and thus would prevent medical treatment guidance.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

Individuals have the right to consent to the use of EEG information. Consent is obtained verbally at the time of appointment and study acquisition. Individuals who do not provide consent would not be eligible for study acquisition as part of their medical care.

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

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

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

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

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

Follow the format below:
<u>Privacy Risk:</u>
Zeto is not in control how VA collects data from individuals

<u>Mitigation:</u>
Zeto is not in control how VA collects data from individuals

Section 7. Access, Redress, and Correction

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

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

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

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

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

Individuals can gain access to EEG test results by submitting a Release of Information (ROI) form.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Procedures for correcting information is described in *VHA Directive 1605.01, Privacy and Release of Information – Section 8. RIGHT TO REQUEST AMENDMENT OF RECORDS.*

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.

N/A - Zeto is not in control of how VA allows individuals to correct their data. VA personnel can show and edit patient records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.
Mitigation:
Zeto EEG mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records.

Zeto EEG Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate

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.

Zeto does not provide access to any other agency, hence there is no PII sharing.
A simplified role-based access model of VA user vs Super-users is implemented, which limits what PII can be accessed. Implementing a granular role-based access control for controlling read-only access, hiding PII/PHI, is scheduled for Q2 2022.

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.

Contractors will have access to the Area Boundary after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area Boundary only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA Area Albany access must have an approved computer access request on file. The area manager, or designee, in conjunction with the area ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules.

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.

This question is related to privacy control AR-5, Privacy Awareness and Training.

Zeto EEG personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the area Privacy Officer and Information Security Systems Officer during new employee orientation. The Privacy and Information Security Systems Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses:

VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics.

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.***

Not available at the time of completing this form. This request is currently in Package Development Phase of the SaaS Intake Process. Zeto starts the FedRAMP process in Q1 2022, expected IOC is June 2023 for the FedRAMP certified cloud solution. This is a High Impact System.

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.

Zeto Cloud Platform implements a PaaS model. Zeto starts the FedRAMP process in Q1 2022, expected IOC is June, 2023 for the FedRAMP certified cloud solution.Cloud Service Provider, AWS. Hosted within VAEC.

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.

VA has ownership of the data - contract number: 36C24621P1342

- This contract doesn’t state who owns the PHI/PII. Does the VA need something else?

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.

Zeto has ownership of operational data solely related to operational statistics, system load and availability and operation logs. Zeto team will collect ancillary data for supporting the users of the system. This is done to identify and troubleshoot problems in the systems.

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.

AWS as a cloud provider offers a shared responsibility model. AWS has all personnel and technical controls ensuring data privacy. A BAA between AWS and Zeto allows utilizing these controls and ensures that data stored at AWS is held private.

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).

No such technology is in use.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MARIE J. MONTAMABADOU 1492273

Digitally signed by MARIE J. MONTAMABADOU 1492273
Date: 2022.07.01 13:28:52 -04'00'

Privacy Officer, Marie Montamabadou

YVONNE GOUDY-BERMUDEZ

Digitally signed by YVONNE GOUDY-BERMUDEZ
Date: 2022.07.01 13:32:13 -04'00'

Information Systems Security Officer, Yvonne I. Goudy-Bermudez

FRED TOLLEY

Digitally signed by FRED TOLLEY
Date: 2022.07.05 10:54:11 -04'00'

Information Systems Owner, Fred Tolley

APPENDIX A-6.1

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

https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false