Privacy Impact Assessment for the VA IT System called:

ID.me -Enterprise

Department of Veteran's Affairs
VA Central Office

Date PIA submitted for review:

09/02/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	(202) 632-8431
Information System Security Officer (ISSO)	Brian Kohler	Brian.Kohler@va.gov	(412) 822-3272
Information System Owner	Herbert Ackermann	Herbert.Ackermann@va.gov	(202)-461-0543

Abstract

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

ID.me is a Software as a Service (SaaS) cloud solution that provides a form of two factor authentication that credentials users into VA space. The tool is intended to provide credentials for external users who do not have VA accounts with VA.gov, Single Sign On External (SSOe/AcessVA), Application Programming Interface (API), and Cerner Electronic Health Record Modernization (EHRM). The users include veterans, VA employees and contractors. The user, who has shared the credentialing information with ID.me, attempting to gain access to VA space will pass a Security Assertion Markup Language (SAML) authentication token that ID.me holds to the VA for authentication, and once authenticated, passes it back to the user to allow them access to the VA space. This is an automatic authentication flow that happens through a user's browser and is compliant with the SAML standard that can be found at https://tools.ietf.org/html/rfc7522.

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?*

ID.me -Enterprise falls under the VA Central Office–OIT.

The purpose of the system is to allow VA personnel to credential users into VA space using a form of two factor authentication. This will be especially helpful for work done with partners who do not have VA accounts. ID.me provides a complete identity platform featuring NIST 800-63-3 IAL2 & AAL2 aligned capabilities for

online and in-person identity verification. The platform brings together best-in-class identity and fraud capabilities into a comprehensive, easy-to-deploy solution.

No third-party organizations have direct access to the PII. However, the PII is used by the ID.me Identity Gateway system to validate an individual's identity with Credential Service Providers and Identity and Attribute data sources through application-level data calls, such as an Application Programming Interface (API). Any information transmitted to a third-party identity proofing organization uses industry standard encryption tools, designed to protect the PII information from unauthorized access.

The expected number of individuals that use ID.me is synonymous to the number of veterans, veteran dependents, VA employees, contractors, volunteers, and clinical trainees. As this number is in constant flux, so to is the number of potential users.

The ID.me Vice President of Security and Risk Management has the ultimate responsibility for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system. ID.me has in place applicable physical, managerial and technical procedures designed to safeguard and secure the PII information retained in the system. In addition, all sensitive information supplied by the customer is encrypted at rest and in transit.

The SSN is used in the identity proofing process ID.me provides for VA. This is required by NIST SP 800-63-3 and VA Directive 6510. The legal authority to use and collect SSNs to support digital identities is provided through:
Title 44 United States Code Section 3551-3558
Federal Information Security Modernization Act (FISMA) of 2014 Title 5
United States Code Section 522(a).

The two SORNs that allow ID.me to collect personal information such are: 150VA19 and 138VA005Q

Completion of the PIA will not result in changes to the business process.

Completion of the PIA will not result in technology changes.

The system is not in the process of being modified. It is a commercial off the shelf system (COTS) Software-as-a-Service (SaaS). ID.me does use cloud technology and has FedRAMP authorization.

ID.me Privacy Policy specifically states that "… the decision to share specific items of the customer's Personally Identifiable Information and/or Sensitive Information with the ID.me Service is the customer's and the customer's alone. The user can elect to provide all or only some of the information requested by the Website during the registration process and at any time they may decide to remove some of the information that they previously provided." The user retains complete ownership of the PII they place on the system. [Because this information/data is used to authenticate users within the VA with VA systems, the data is owned by VA.]

FedRAMP upholds ID.me to NIST 800-144 requirements regarding the accountability of security and privacy of data being held.

Information that contains PII, should it become compromised, could potentially have serious impact on the reputation of the Veterans Affairs. This could also cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced. This could potentially also result in significant damage to organizational

assets or result in significant financial loss. The compromise of data could potentially also result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. If an individual's privacy related data is disclosed, it could result in a fraudulent act or identity theft by an unauthorized individual.

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)

Self-taken Camera Picture "selfie", User ID, Healthcare Provider Status, My HealtheVet (MHV) UUID, DSLogon UUID – EDIPID, DSLogon – Deceased Indicator, DSLogon – User Status, (Sponsor/Dependent)

PII Mapping of Components

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

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

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
Database Servers	Yes	Yes	• Full Name • Social Security Number • Address • Phone Number • Email Address • Driver's License Number • Passport Number • Date of Birth • Gender • Integration Control Number (ICN) • Self-taken Camera Picture "selfie" - No longer captured as of 09MAY22 per the request of the VA • User ID • Healthcare Provider Status • My HealtheVet (MHV) UUID	Electronically verify individual's identity for Relying Party	Internal AWS Security Group, multifactor authentication, encryption, continuous monitoring

			• Mother's Maiden Name • DSLogon UUID – EDIPID • DSLogon – Deceased Indicator • DSLogon – User Status (Sponsor/Dependent)		
Application Servers	Yes	No	• Full Name • Social Security Number • Address • Phone Number • Email Address • Driver's License Number • Passport Number • Date of Birth • Gender • Integration Control Number (ICN) • Self-taken Camera Picture "selfie" - No longer captured as of 09MAY22 per the request of the VA • User ID • Healthcare Provider Status • My HealtheVet (MHV) UUID • Mother's Maiden Name • DSLogon UUID – EDIPID • DSLogon – Deceased Indicator DSLogon – User Status (Sponsor/Dependent)	Electronically verify individual's identity for Relying Party	Internal AWS Security Group, multifactor authentication, encryption, continuous monitoring
Storage and Backup	Yes	Yes	• Full Name • Social Security Number • Address • Phone Number • Email Address • Driver's License Number	Electronically verify individual's identity for Relying Party	Internal AWS Security Group, multifactor authentication, encryption, continuous monitoring

			• Passport Number • Date of Birth • Gender • Integration Control Number (ICN) • Self-taken Camera Picture "selfie" - No longer captured as of 09MAY22 per the request of the VA • User ID • Healthcare Provider Status • My HealtheVet (MHV) UUID • Mother's Maiden Name • DSLogon UUID – EDIPID • DSLogon – Deceased Indicator DSLogon – User Status (Sponsor/Dependent)		

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

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

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

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

The information from Section 1.1 is provided directly by the individual creating the account.

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.

ID.me collects the information from the individual – the user can use various forms of identity verification when creating their account:

NIST 800-63-2 LOA3 (96% of VA users) - For identity verification, NIST provides guidance on two possible pathways and ID.me offers both:

a. Document-based. Requires the verification of a government issued ID (Driver's License, Passport, Passport Card, or State ID) combined with verification of utility and financial records via the user's phone number and SSN.

b. Knowledge-based. Confirmation of user's PII within credit records, known as Knowledge-Based Verification (KBV) combined with verification of utility and financial records via the user's phone number and SSN.

NIST 800-63-3 IAL2/AAL2 via Supervised Remote (4% of VA users) - To adhere to the NIST requirements for evidence collection, ID.me offers two options in the supervised remote pathway:

c. One piece of strong evidence (e.g., government-issued ID) and two pieces of fair evidence (e.g., utility bill and financial record check) or,

d. Two strong pieces of evidence (e.g., Driver's License and Passport).

After an account is created the ID.me login credential is used to sign into any websites that will need identity verification.

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.

The main function of the ID.me Identity Gateway is to verify an individual's identity based on the information provided (provided as explained in Section 1.3). To accomplish this, the system verifies that the information contained in the system is current and accurate each time that Identity Proofing of the individual occurs. The individual can change, correct or amend their information in the system at any time using the website account.

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

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

The SSN is used in the identity proofing process ID.me provides for the VA. This is required by NIST SP 800-63-3 and VA Directive 6510. The legal authority to use and collect SSNs to support digital identities is provided through:

- Title 44 United States Code Section 3551-3558
- Federal Information Security Modernization Act (FISMA) of 2014
- Title 5 United States Code Section 522(a).

The two SORNs that allow ID.me to collect personal information such are:

- 150VA19
- 138VA005Q

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.

Follow the format below when entering your risk assessment:

Privacy Risk: Privacy risks revolved around a loss of control, unauthorized access, and excessive access to an individual's PII. However, the entire purpose of ID.me is to authenticate a user,

which requires the use of PII for the VA. The current data collected is directly necessary to accomplish the purpose to verify access authorizations. All data is collected directly from the individual. The data's accuracy and completeness is verified dependent upon the method an individual chooses to create the account and is described in Section 1.3.

Mitigation: Collection of data is limited only that which is required to verify an individual's access authorizations – this is dependent upon the method a user chooses to create an account as described in Section 1.3. All ID.me personnel with access to the data must first authenticate to the system and an audit trail is generated when the database is accessed. These audit trails are reviewed by the Information System Security Officer and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken.

There are several mitigating controls to help manage the privacy risks mentioned above:

1. All sensitive personally identifiable information is encrypted prior to storage within the database. The layer of encryption prevents those with system-level access from reading/extracting the information stored therein.
2. All access to production systems is controlled through multi-factor authentication and VPN connectivity to the environment to ensure only legitimate users are permitted to access the systems.

All access to production is logged and audited to identify misuse or unauthorized access to sensitive information

Section 2. Uses of the Information

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

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

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

The main function of the ID.me Identity Gateway is to verify an individual's identity based on the information provided. In order to accomplish this, the system verifies that the information contained in the system is current and accurate each time that Identity Proofing of the individual occurs.

- **First and Last Name** —Collected by ID.me as part of the minimum attributes necessary to accomplish identity verification
- **Social Security Number**—Collected by ID.me as part of the minimum attributes necessary to accomplish identity verification
- **Personal Mailing Address**—Collected by ID.me to resolve and validate the claimed identity

- **Personal Phone Number(s)**—Collected by ID.me to validate the claimed identity exists in the real-world and is reasonably associated with the real-world identity.
- **Personal Email Address**—Collected by ID.me as part of the minimum attributes necessary to accomplish identity verification
- **Certificate/License numbers**—Collected by ID.me to resolve and validate the claimed identity
- **Passport Number**—Collected by ID.me to resolve and validate the claimed identity
- **Date of Birth**—Collected by ID.me as part of the minimum attributes necessary to accomplish identity verification
- **Gender**—Collected by ID.me to resolve and validate the claimed identity
- **Integration Control Number (ICN)** — the VA sends the ICN tied to MyHealtheVet (MHV) accounts to ID.me to resolve and validate a user
- **Self-taken Camera Picture** "selfie" — Collected if the claimed identity chooses to verify their identity via Supervised Remote verification process. (Discontinued on 09 May 2022 at the request of the VA.)
- **User ID**—Collected by ID.me to resolve and validate the claimed identity
- **Healthcare Provider Status**—Collected by ID.me to resolve and validate the claimed identity
- **Mother's Maiden Name**—Collected if the claimed identity chooses to verify their identity via Knowledge-Based Verification
- **DSLogon UUID (EDIPID) —**Collected by ID.me to resolve and validate the claimed identity
- **DSLogon – Deceased Indicator—**Collected by ID.me to resolve and validate the claimed identity
- **DSLogon – User Status (Sponsor/Dependent)** —Collected by ID.me to resolve and validate the claimed identity

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

All information is provided by the individual for the purpose of electronic identity verification. The information is analyzed by the ID.me Identity Gateway system to validate an individual's identity with Credential Service Providers and Identity and Attribute data sources are through application-level data calls, such as an Application Programming Interface (API). Any information transmitted to a third-party

identity proofing organization uses industry standard encryption tools, designed to protect the PII information from unauthorized access.

2.3 How is the information in the system secured?

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

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

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

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

All user data, including personal information such as SSNs, are stored on AWS using FIPS 140-2 validated encryption. Prior to storage, data is encrypted with an encryption appliance then sent to the storage area, S3 or EBS, where it is then encrypted again. While traversing the network, internally or externally, TLS 1.2 or greater encryption is used for all traffic.

PII/PHI is also safeguarded via access control; access to PII is granted only to an individual with a valid job function that requires access to the data - only authorized and trained ID.me engineers/system administrators and customer support personnel have access to the data within the database that houses the PII. ID.me enforces approved authorizations for logical access to resources using the Palo Alto VPN for privileged users and the Imperva Web Application Firewall for application end-users. The Palo Alto VPN is used to establish an ID.me privileged user connection to IDIG servers. The VPN uses a static public IP address assigned by AWS. Once System Administrators are connected to the VPN, they can connect via Secure Shell (SSH). Multi-factor authentication is configured for access to the VPN gateway that provides privileged users with access to IDIG servers. The Palo Alto VPN is the single point of entry for all privileged administrators connecting to the IDIG production environment.

2.4 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.

Add answer here:

Access to PII is granted only to an individual with a valid job function that requires access to the data. All system access to any aspect of the ID.me Identity Gateway requires manager approval, as well as the formal issuance of access credentials and authenticators. Only authorized and trained ID.me engineers/system administrators and customer support personnel have access to the data within the database that houses the PII. Engineers/System Administrators require access to the database in order to maintain the system. Customer support personnel require access to the customer's data to resolve customer support questions and issues.

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

ID.me retains both information within the system and output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements in accordance with the ID.me FedRAMP Policies and Procedures.

- Full Name
- Social Security Number
- Address
- Phone Number
- Email Address
- Certificate/License numbers
- Passport Number
- Date of Birth
- Gender
- Integration Control Number (ICN)
- Self-taken Camera Picture "selfie" - No longer captured as of 09MAY22 per the request of the VA
- User ID
- Healthcare Provider Status
- Mother's Maiden Name
- My HealtheVet (MHV) UUID
- DSLogon UUID – EDIPID
- DSLogon – Deceased Indicator
- DSLogon – User Status (Sponsor/Dependent)

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.

Data is retained after account closure for up to three years. Users may request that ID.me delete certain Personal Information at any time at account.ID.me or through the ID.me Privacy Rights Center, where applicable. However, ID.me reserves the right to retain data tied to certain high-risk transactions, particularly in government and healthcare settings, exclusively for fraud prevention and government audit purposes.

A user can also close their account at any time which will initiate the process to remove individual data. The user will (1) sign in, (2) select to close their account, and (3) confirm account deletion. Seven days following confirming account deletion, the account and its associated data will be purged from ID.me. The user may contact ID.me Member Support within seven days to reactivate the account. As noted in the Privacy Policy, an individual's PII may be retained in database backups for up to the maximum retention rate.

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.

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

3.4 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

PII is automatically decommissioned when the last backup containing the information is retired. If the storage device storing the data is decommissioned by AWS, it is sanitized by AWS in accordance with AWS's FedRAMP media sanitization procedures.

Once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system, they are wiped clean and the data overwritten.
Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014),
https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf

In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA.

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

ID.me does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information
Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that PII is retained for longer than it is useful.

Mitigation: All user data, including their personal information such as SSNs, is stored on AWS using FIPS 140-2 validated encryption. Prior to storage, data is encrypted with an encryption appliance then sent to the storage area, S3 or EBS, where it is then encrypted again. While traversing the network, internally or externally, TLS 1.2 or greater encryption is used for all traffic.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Digital Experience Product Office (DEPO) / Office of Chief Technology Officer (OCTO)	To verify user identity on signed documents and projects	User Id, First Name, Middle Name, Last Name, SSN Gender, Date of Birth, Phone Number, Email Address Street, City, State, Postal Code	Security Assertion Markup Language (SAML) response/ token over Transport Layer Security/Secure Socket Layer (TLS/SSL)
My HealtheVet	To verify user identity on signed documents and projects	User Id ICN MHV Account Type MHV Available Service Information	SAML response/ token over TLS/SSL
Identity and Access Management (IAM)	To verify user identity on signed documents and projects	User Id, First Name, Middle Name, Last Name, SSN Gender, Date of Birth, Phone Number, Email Address Street, City, State, Postal Code	SAML response/ token over TLS/SSL
Project Special Forces	Lighthouse API	User Id, First Name, Middle Name, Last Name, SSN Gender, Date of Birth, Phone Number, Email Address Street, City, State, Postal Code	SAML response/ token over TLS/SSL

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 the data, and SSN, could be shared with an inappropriate VA organization or institution

Mitigation: The potential harm is mitigated by access control, configuration 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, program management, planning and maintenance. There is required HIPAA training for users of the system, and PII/PHI is on a need to know basis. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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*
N/A				

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: Disclosure of personally identifiable information, that if disclosed may expose the respondent/subject to financial loss or identity theft. Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety.

Mitigation: All third parties in receipt of personally identifiable information have signed contracts and confidentiality agreements with ID.me, Inc. Information shared during the course of business and reporting has also been consented to by the end user as part of onboarding to the designated third party or services (e.g. sharing of PII with Veteran's Affairs). Access to PII internally is only granted to employees with proper training and on a need-to-know basis to limit exposure to PII.

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.

A privacy notice is provided to users. It is replicated in completion as Appendix B.

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 can elect to provide all or only some of the information requested by the system during the registration process, and at any time they may decide to remove some of the information that was previously provided. Disclosure is voluntary, so a user can choose not to provide the PII; however, in doing so, the ID.me Identity Gateway application may not be able verify their identity. In addition, as discussed below, an individual can opt out of the service entirely, resulting in the individual's account and associated PII removal from the system.

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

Yes, users are provided notice and a number of choices about the collection, use, and disclosure of their Personal Information. The specific screens that users will encounter depends upon the type of ID.me credential they are seeking, and the elements of information that ID.me must collect to comply with the requirements of the relevant partner. ID.me never sells user data or shares user data without their explicit consent.

For the VA, users will be prompted with the following consent screens:

- Privacy Policy: First, users are asked to agree to ID.me's Privacy Policy, as well as its Terms and Conditions. Users must check a box to agree to the Privacy Policy and Terms and Conditions. Users may not create an account without agreeing to the Privacy Policy,

which describes processing activities that are necessary for ID.me to provide its products and services. ID.me's Privacy Policy governs all Personal Information collected by ID.me.

- Sharing of Personal Information with Partners: To provide users additional control over their data, ID.me prompts the user to "Allow" verified identity information to be shared with each applicable partner. The data elements vary by partner but typically are disclosed on a consent screen that invites users to "Allow" or "Deny" the relevant data sharing. For example, if a user verifies their identity at VA, ID.me will surface a consent screen with the identity information that will be shared with VA if they click "Allow". If the user clicks "Deny", ID.me will not share the information with VA.

Users may review and manage which partners have access to their verified identity information through their ID.me account settings. A user may opt to allow more than one ID.me partner to access their personal information if they have used ID.me for identity proofing or group verification for more than one partner.

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: Risk that individual is unaware that their information is being collected by the system.

Mitigation: User is made aware at various times during the application process. No federal agencies or other organizations have access to the PII data and, per the Privacy Policy, this information is not shared without the individual's permission. All PII is under the control of ID.me

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 can change, correct, or amend their information in the system at any time using the website account.

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 user owns the data and can contact ID.me directly for support for erroneous information. The individual can change, correct or amend their information in the system at any time using the website account. Additionally, the user can contact the ID.me support to correct any misinformation.

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.

PII collected is verified for accuracy. The main function of the ID.me Identity Gateway is to verify an individual's identity based on the information provided. In order to accomplish this, the system verifies that the information contained in the system is current and accurate each time that Identity Proofing of the individual occurs.

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.

Redress is provided by ID.me in that he individual can change, correct or amend their information in the system at any time using the website account.

Redress is also provided through VA policy. VA Handbook 6300.4-Procedures for Processing Requests for Records Subject to the Privacy Act.

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 individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

Mitigation: Individuals are immediately able to reach out to the local admin for correction purposes. Users may also go to the ID.me website 24/7 to correct the information.

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.

ID.me system access is retained by the ID.me vendor. Access controls are documented within the FedRAMP approval SSP, section 13.

ID.me enforces approved authorizations for logical access to resources using the Palo Alto VPN for privileged users and the Imperva Web Application Firewall for application end-users. The Palo Alto VPN is used to establish an ID.me privileged user connection to IDIG servers. The VPN uses a static public IP address assigned by AWS. Once System Administrators are connected to the VPN, they can connect via Secure Shell (SSH). Multi-factor authentication is configured for access to the VPN gateway that provides privileged users with access to IDIG servers. The Palo Alto VPN is the single point of entry for all privileged administrators connecting to the IDIG production environment.

All access to systems in the IDIG environment must be explicitly authorized following the principle of "least privilege". Authorization includes security related functions such as establishing system accounts and configuring access authorizations (permissions, privileges).

The following system access is defined for the IDIG:

- Web Applications – Application users only have access to run the application functionality through the web services. Users do not have the ID.me Administrator access or access to the AWS Console or resources.
- IDIG Administrator Access – Only privileged ID.me users have ID.me Administrator access. Privileged user duties are separated as follows:
    - System Administrators - Access to manage the operating systems, databases, storage and other AWS resources using the AWS Management Console and/or SSH. System Administrators access is limited to the Web/Application Tier and the Services/Database Tier.
    - VPN Administrator – Access to manage and configure the VPN used by privileged users to connect to the VPC.
    - NetSec Operations Team – Access to manage and configure the security tools and applications in the Security Tier and the Firewall/DMZ Tier.

- Auditor – Access to review and manage the audit logs that are maintained in the Security Tier.

- AWS Management Console – ID.me has implemented AWS IAM policy roles and individual user accounts for separation of duties. IAM policies are attached to the users, enabling centralized control of permissions for users under ID.me's AWS Account. Security functions within the AWS infrastructure can be explicitly defined by the Director Security within IDIG environment to include read-only permissions and authorized user functions Access to Splunk, Tenable Security Center, and other tools is limited to only IDIG Director Security and IDIG staff based on need-to-know and access granted based on least privilege.

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

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

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

Yes, the target user population for ID.me is any user requiring identity verification, potentially the entire Veteran population, their dependents, VA's customers and business partners including but not limited to contractors and other users to the information system. But all users will only have access to their own PII.

Contractors are required to complete the same provisioning, onboarding and training requirements as all VA users prior to access to VA Information Systems. VA COR review and manage contracts and non-disclosure agreements approved by VA. The COR oversees the contracts awarded to contract personnel. No Contractor access to information system is granted without VA COR approval.

No contractor, volunteer, or employee has any access to VA information systems and PII until they have been fully on boarded. Contractors as well as VA employees receive annual training regarding their roles on the system and sign a "Rules of Behavior for EP" that prevents VA contractors from using PII in any manner not consistent with business needs. Administrators ensure screening is conducted for all contract personnel and federal employees and all other appointed workforce members. The onboarding process consists of screening, as defined by VA Directive and Handbook 0710 Personnel Suitability and Security Program, of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required.

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

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

All VA users of ID.me are required to complete annual Privacy Security Training, as well as VA Rules of Behavior training and VA mandated privacy HIPAA training

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

Yes.

If Yes, provide:

1. *The Security Plan Status,* Approved
2. *The Security Plan Status Date*, 07 Dec 2020
3. *The Authorization Status,* Authorization to Operate (ATO)
4. *The Authorization Date*, 18 Mar 2021
5. *The Authorization Termination Date*, 21 Jan 2024
6. *The Risk Review Completion Date,* 10 Mar 2021
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH), Moderate

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.***

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.

ID.me -e uses FedRAMP authorized cloud technology with a Software as a Service (SaaS) model.

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.

The VA contracts with ID.me under Contract Number NNG15SD27B. Section 6.a states that any "information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract…shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA."

ID.me's purpose is to support authentication of users. Any data collected ultimately is owned by the user who provides the data; the user may request deletion of associated data at any time and the data will be removed as described in previous sections.

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.

Only data used to support authentication of user is collected as described in previous sections. The user retains ultimate ownership of the PII they provide to ID.me. Since this data is used to authenticate users within the VA with VA systems, some of the data may also be owned by VA.

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.

This principle is described within the VA contract NNG15SD27B with ID.me. In addition to language requiring specific information security training and security requirements, Section B.5.6.c is "A requirement to pay liquidated damages in the event of a data breach" which displays the accountability ID.me has for the data held within its system.

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).

RPA is not used in ID.me.

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

ID	Privacy Controls
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.09.08 07:04:35 -06'00'

Privacy Officer, Julie Drake

Brian R Kohler 290480

Digitally signed by Brian R Kohler 290480
Date: 2022.09.07 15:57:01 -04'00'

Information System Security Officer, Brian Kohler

HERBERT ACKERMANN

Digitally signed by HERBERT ACKERMANN
Date: 2022.09.08 07:26:34 -04'00'

Information System Owner, Herbert Ackermann

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).

150VA19:

https://www.oprm.va.gov/docs/CurrentSORNList_7_24_20.pdf

138VA005Q:

https://www.oprm.va.gov/docs/CurrentSORNList_7_24_20.pdf

ID.me Privacy Policy: https://wallet.id.me/privacy

Appendix B – ID.me Privacy Policy

PRIVACY POLICY

Version: 6.5.1

Last updated: 2022-06-29

ID.me Privacy Bill of Rights

ID.me Privacy Statement

ID.me will not sell, rent, or trade your Personal Information. ID.me will only transfer your Personal Information at your request, and with your consent, for use by third parties to verify your identity or group eligibility, and as required for the prevention of fraud. ID.me has built rigorous security and privacy requirements into our technology from inception. We are an ethical steward of your Personal Information and are committed to supporting the following principles:

- ***You** are solely in control of your own Personal Information.*
- ***You** must provide consent before we will share any of your Personal Information.*
- ***You** can see all authorized applications and which specific elements of your Personal Information are shared in your My Account portal.*
- ***You** can revoke access to your Personal Information for any authorized app at any time.*
- ***You** may destroy your ID.me credential and disallow for further external use of any associated Personal Information at any time.*

ID.me Privacy Policy

This Privacy Policy describes how ID.me and its affiliates (collectively "ID.me") collect, use and disclose certain information, including your Personal Information, both online and offline, and the choices you can make about that information. We respect your concerns about privacy, and value our relationship with each of our users – it is for this reason that ID.me will never sell, rent, or trade your Personal Information, and why we take measures to safeguard your Personal Information as we work to become the identity verification layer of the internet.

When you verify yourself using ID.me, through our mobile and online applications, use our in-person verification tools or other products and services, visit our websites, view our content, or contact our customer service (collectively, the "Services"), we may collect information from or about you. There may be additional notices about our information practices and choices for certain ID.me levels of verification, including our Biometric Information Privacy Policy. By using any of the Services, you acknowledge the data collection practices and purposes outlined in this Privacy Policy. You can learn more about ID.me

and our affiliates by visiting the About ID.me section of our website, or by reviewing any of our whitepapers.

Click on each header below for more information or scroll down to read the full policy.

1. What Information We Collect About You

We collect information from and about you in connection with your use of the Services. Some of this information may be considered "Personal Information" which is information that identifies you or your device, or is reasonably associated with you. The categories of Personal Information we may collect will vary depending on the nature of the Service you choose.

We also collect, use, and disclose aggregated or de-identified information that does not reasonably identify you or your device, and is not considered Personal Information.

Information You Provide

We Collect Information You Provide to Us Which Includes:

Verification information. When you verify yourself, either individually or as part of a group, with ID.me you provide us with Personal Information that may include your name, date of birth, social security number and/or other government issued identification numbers, copies of your government issued identification card (e.g., license or passport), email address, phone number, mailing address, and certain photographic images, and biometric data. You may also be asked to provide group affiliations (e.g., Military, First Responder, Student, Veteran, etc.), memberships, educational degrees, and professional certifications.

Please note, ID.me asks that you not provide physical documentation, via mail service or otherwise, to ID.me. All documentation to be collected should be provided either through the ID.me app or website portal, or presented to a trusted referee where applicable.

Your correspondence and your feedback about our Services. We collect information you provide when you contact us directly or provide feedback, comments, or suggestions on our Services directly to us.

Information you provide when you do business with ID.me. If you are a vendor, service provider, or business partner of ID.me, we may collect information about you and the services you provide, including your or your employees' business contact information and other information you or your employees provide to us as part of the services you may provide and our agreement with you.

Information you provide offline. You may also provide information to us in person and offline. You may be recorded if you visit our offices (including by security surveillance of our premises, including CCTV).

Other information. We also collect information that relates to or is capable of being associated with you, such as age, gender, and any other information you choose to provide.

Information Collected Automatically

When using our Services we may automatically collect or receive certain information associated with you or your network device(s), such as your computer or mobile devices. This includes information about your use of our Services and your preferences. Such information may be automatically collected through device-based tracking technologies such as cookies, pixels, tags, beacons, scripts, or other technologies. For more information about cookies or other tracking technologies and the choices you have regarding the use of them, please visit our ID.me Cookie Policy.

The information we automatically collect may also include geolocation information, such as information that identifies the approximate location of your device and your IP address, which may be used to estimate your approximate location.

Information from our partners. We acquire information from other trusted sources. These business partners might include companies, such as your mobile phone carriers, certain government agencies, licensing bodies, etc. We may also collect information about you from other sources, including service providers, data licensors and aggregators, marketing companies, programming distributors, and public databases.

Information you provide through social media

If you connect to us through a social media platform or navigate to a social media platform from one of our sites, the social media platform will collect your information separately from us. You should review the social media platforms' privacy policies to understand how they are using your information and your rights in relation to such information.

Information We Derive

We may derive additional information or draw inferences about you based on the information we have collected from you directly, passively, or through third parties.

2. How We May Use Your Information and Why

ID.me will not sell, rent, or trade your Personal Information. ID.me will only transfer your Personal Information at your request, and with your consent, for use by third parties to verify your identity or group eligibility, or as required for the prevention of fraud or otherwise permitted by law.

We may use information to provide you with our Services. We may use the information collected from or about you to authenticate and manage your identity when you create an ID.me account, including to verify attributes of your identity including, but not limited to, group affiliations (e.g., military status, first responder, student, veteran status, etc.), memberships, social media accounts, educational degrees, and professional certifications, as well as to provide you with customer support and account updates. We may use this information to verify your identity with ID.me partners in both the public and private sector at your request and perform our contractual obligations with you or to ensure that our Services function properly.

We may use information to perform our contracts with you. If ID.me enters into a contract with you, including in instances where you may be a vendor or service provider to ID.me or our business partner, we may use your information to fulfill our contractual obligations.

We may use information for marketing purposes. If you have opted into receiving marketing communications, then we may use your information to send promotional messages and newsletters via email, or otherwise alert you to products or Services we think might be of interest to you, including for the ID.me Shop. You may unsubscribe from receiving marketing communications from us at any time by logging in to your account and navigating to "My Preferences" to manage your subscriptions.

Please note, if you are using ID.me Services in connection with legal identity verification for a state or federal government agency we will not use any Personal Information provided as part of your verification for any type of marketing or promotional purposes.

We may use information to improve our Services. We use your information to monitor and improve the operation, delivery, and general accessibility of our Services. This may also include conducting internal research and development of our Services.

We may use information to maintain the safety and security of our Services. We may use your information to protect the rights and property of ID.me and others, and to comply with our legal obligations including to detect, investigate, and prevent fraud and other illegal activities and to enforce our agreements.

We may use information as otherwise permitted by law. We may use your information to resolve disputes, enforce our agreements, and as otherwise permitted or required by law.

We may use your Biometric Information. We may use your Biometric Information to verify your identity for certain partners, such as the Internal Revenue Service (IRS) or various other federal or state agencies (e.g., Department of Labor or Division of Unemployment Benefits), as well as to detect and help prevent fraud. We also may use the information in other ways with your consent, such as when you choose to use a Service or participate in a program we may offer jointly with another entity. We will never sell, rent, or trade your Biometric Information.

For additional information on how ID.me collects an, uses, and protects your Biometric Information, please see our Biometric Information Privacy Policy.

Additional Information regarding the Service Member Civil Relief Act (SCRA). In order to better serve members of America's Armed Forces and other personnel covered by the Service Members Civil Relief Act (SCRA) (50 U.S.C. App. 501 et. seq.), ID.me provides services to Financial Services companies and third party websites in order to facilitate their compliance with the provisions of SCRA. By joining ID.me, you agree that ID.me may use your Personal Information in order to assist Financial Services companies and third party websites so they may determine your eligibility or your family member's eligibility for SCRA benefits and protections. ID.me may periodically use your Personal Information to confirm your SCRA eligibility or your family member's eligibility at a later point in time to inform third parties of any changes so they may determine continued eligibility for SCRA benefits and protections. Sources of this information may include, but are not limited to, publicly available websites, physical documentation, financial information, ID.me's network or third parties that have a relationship with ID.me.

The scope of ID.me's SCRA services includes all individuals protected by the SCRA (i.e. personnel serving in the United States Armed Forces, commissioned officers of the Public Health Service and the National Oceanic and Atmospheric Administration, U.S. citizens serving with the armed forces of nations allied with the United States, and, where applicable according to federal or state laws and regulations, dependents and family members of an individual protected under the SCRA.

3. Who We Share Your Information With and Why

ID.me will not sell, rent, or trade your Personal Information. ID.me will only transfer your Personal Information at your request, and with your consent, for use by third parties to verify your identity or group eligibility, or as required for the prevention of fraud or otherwise permitted by law.

We may share your Personal Information with entities necessary to validate your ID.me Account and provide our Services to you. In order to verify your identity and eligibility to receive discounts and other benefits from our partners and other service providers, we may provide your Personal Information to third parties such as government agencies, telecommunications networks, financial institutions or other trusted and reliable sources of information. Our provision of your Personal Information to the foregoing parties is solely to verify your identity and eligibility for ID.me Services. We have established relationships with Registration Authorities similar to the entities described above whereby the Personal Information you provide to us will be transmitted to them using industry standard encryption tools, designed to protect such information from unauthorized access.

We may share your information in connection with a corporate transaction. We may disclose or transfer your information as part of, or during negotiations for, any purchase, sale, lease, merger, or any other type of acquisition, disposal, or financing involving our brands.

We may share information with third parties who perform services on our behalf. We may share your information with unaffiliated companies or individuals we hire or work with that provide us with

professional advice, business support, or perform services on our behalf, including customer support, web hosting, information technology, payment processing, direct mail and email distribution, and administration, and analytics services. These Service Providers are allowed to use your information to help us provide our Services and not for any other purpose.

We may share information as needed in order to comply with legal processes, to protect ourselves, or improve our Services. For example, we will share information when it is necessary for us to comply with applicable law or legal process, to respond to legal claims, to prevent fraud, or to protect our rights or the property or personal safety of our users, employees, or the public.

We also use third party service providers to track and analyze website usage and volume statistical information to administer our Website and constantly improve its quality.

We may share information as required with the United States federal government and certain state governments. ID.me does not provide any government with direct and unfettered access to our user's data, and we do not provide any government with our encryption keys or the ability to break our encryption. We may share certain Personal Information associated with an ID.me account with government entities where we reasonably believe that account may be engaging in fraud.

If a government entity requires additional information related to an ID.me account, whether related to a suspected instance of fraud or otherwise, it must follow applicable legal processes. It must serve us with a subpoena, warrant, or present other legally compelling justification for the additional information associated with the account, the request must be targeted and specific in nature.

Our legal and compliance teams review all requests to ensure they are valid, reject those that are not valid, and only provide the data specified in the subpoena or similar court order.

4. Your Choices, Rights, and Controls

You have certain choices about how we use your information, including how your Personal Information is shared.

Close your ID.me Account. You may close your ID.me account at any time, by choosing to close your ID.me account you are directing ID.me to deactivate your identity credential and to purge the associated data from active use in our databases. Please note, however, that ID.me does retain account history (e.g., events, logins, and transactions) as well as verification history (e.g., group, vaccine, or identity details including documentation and data elements used for verification) for up to three (3) years.

- **Please Note:** Use of your ID.me credential to verify your identity with state or federal government agencies will be stopped in the event you delete your ID.me account. Please check with the specific state or federal government agency associated with your particular use case to confirm whether periodic or ongoing identity verification is required.

Deleting your selfie image and Biometric Information. Users who have created an account requiring submission of a selfie image, and who consented to the collection of the associated Biometric

Information, may request the deletion of both the selfie image and Biometric Information by submitting a request through the ID.me "Privacy Rights Center" which is accessible via a link at the bottom of our Website, or under the "Privacy" setting in your account. Deletion of the selfie image and associated Biometric Information may take up to seven (7) days and will not impact the validity of your credential or verified status. ID.me reserves the right to retain this information as needed to comply with our legal obligations or to help prevent fraud.

Opt out from receiving marketing emails. To stop receiving our promotional emails, follow the instructions in any marketing email you get from us. When applicable, you can also change your preferences in your account. Even if you opt out of getting marketing emails, we are permitted to send you transactional messages. For example, we may still contact you about your use of our Services or any changes to our policies or Terms of Service.

Change or update the information you have given us. If you have verified yourself and created an ID.me account, then you can correct or delete certain information or update your verification information by logging into your account and following the instructions or by contacting the member support team.

Control cookies and tracking tools. To learn how we—and our vendors—use cookies and other tracking tools, please visit the ID.me Cookie Policy.

Ad Choices. We, our affiliates, and any associated third parties may collect information on our Services to help alert you to products and Services that may be relevant to your interests. This is known as interest-based advertising. We rely on third parties who collect information on the Services to provide opt-outs or other controls to you. For more information on how to opt-out of receiving interest-based advertising on desktop and mobile websites, please visit:

- Network Advertising Initiative

5. Updating and Correcting Your Information

Accessing and updating your Personal Information. We believe that you should have the ability to access and edit the Personal Information you provide us. You may change any of your Personal Information by logging into your account and accessing the "My Account" section of the site.

You may update your Personal Information by sending us an email at help@id.me. Please indicate your name, address and email address, and what information you would like to update when you contact us. We encourage you to promptly update your Personal Information if it changes. You may also ask to have the information on your account deleted or removed from active use in our databases; however, we may retain certain information if required by law or by certain credential providers (e.g., the National Institute for Standards and Technology), contractual obligation, or for internal use by ID.me in the prevention of fraud.

6. Privacy Policies of Third Parties

This Privacy Policy applies only to ID.me and our Services. This Privacy Policy only addresses the use and disclosure of information we collect from you on www.ID.me. Other websites, including third party websites, may be accessible through this Website have their own privacy policies and data collection, use

and disclosure practices. If you link to any such website, we urge you to review such website's Privacy Policy. We are not responsible for the policies or practices of third parties.

7. Protecting Your Information

We use reasonable security measures. We are committed to protecting your information. We have adopted technical, administrative, and physical security procedures to help protect your information from loss, misuse, unauthorized access, and alteration. Please note that no data transmission or storage can be guaranteed to be 100% secure.

To safeguard certain sensitive information (such as biometric information and government-issued identification information), we implement security measures such as encryption, firewalls, and intrusion detection and prevention systems.

In addition, the following are examples of security measures that are used to safeguard all types of Personal Information we maintain about our consumers:

- Procedures for the identification and classification of Personal Information and implementation of safeguards appropriate to the sensitivity of the information;
- access control procedures designed to verify a business need before access to Personal Information is granted, and procedures for the periodic review of access permissions;
- procedures for termination of access to Personal Information designed to curtail access to the information by terminated personnel or when there is no longer a business need for access;
- personnel security controls designed to reduce the risk of human error, theft, fraud or misuse of facilities; and
- physical and environmental security procedures designed to prevent unauthorized access, damage or interference to business premises and information.

8. Data Retention

Personal Information will be retained until we have fulfilled our legal, contractual and policy obligations. ID.me stores your Personal Information for as long as needed, or permitted, based on the reason why we obtained it (consistent with applicable law and contractual obligations). This means we may retain your Personal Information even after you close your account with us, for up to three (3) years. Users may request that ID.me delete certain Personal Information at any time at account.ID.me or through our Privacy Rights Center, where applicable. We acknowledge all such requests, however we reserve the right to retain data tied to certain high-risk transactions, particularly in government and healthcare settings, exclusively for fraud prevention and government audit purposes.

ID.me aligns to the National Archives recommended guidelines for data retention when supporting government agencies. Personal Information provided by users in connection with a public sector agency as part of their verification may be retained for up to three (3) years after account closure, unless applicable regulations require a shorter retention period.

Selfie Image and Associated Biometric Information. Certain pieces of Personal Information, such as a selfie image and the associated Biometric Information submitted by users for certain types of verification Services, are retained in line with ID.me's obligations to our partners, with the specific retention periods determined by the first partner with whom a user first verifies their identity (e.g., IRS, Dept. of Veterans Affairs, etc.) Certain partners may require this information to be purged within twenty-four (24) hours following a successful verification, other partners may require a longer retention period, but under no circumstances will ID.me this retain information for longer than thirty-six (36) months absent a subpoena, warrant, or other legally compelling justification.

While we store your Personal Information, we use approved industry-recognized encryption methods to protect it from unauthorized access. Likewise, when we destroy your Personal Information, we use industry-recognized methods to affect such destruction.

9. Children's Privacy

We do not knowingly collect information from minors. Minors under the age of 18 may not use the Website. We do not knowingly collect Personal Information from anyone under the age of 18, and no part of the Website is designed to attract anyone under the age of 18. Because we do not intentionally collect any information from children under the age of 18, we also do not knowingly distribute such information to third parties. If you have reason to believe that a child under 18 years of age has provided us with information, please contact us at support@id.me and we will immediately delete such information, subject to and in compliance with applicable law.

10. Additional Information If You Are Located In California

Residents of California. Pursuant to the California Consumer Privacy Act of 2018 (CCPA), residents of California are entitled to additional rights and disclosures regarding their Personal Information. Please see our Notice to California Residents for additional information regarding these disclosures and how to exercise your rights.

11. Additional Information If You Are Located in Europe

This Website is hosted in the United States. If you are a User accessing our Website from Europe, Australia, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States' laws, you are transferring your Personal Information to the United States which does not have the same data protection laws as such other regions. By providing your information to the Website, you are consenting to the transfer of your information to the United States for processing and maintenance in accordance with this Privacy Policy and our Terms of Service. You are also consenting to the application of Delaware law and controlling U.S. Federal law in all matters concerning the Website and ID.me Service.

12. Biometric Personal information

ID.me will not sell, rent, or trade your Personal Information. ID.me will only transfer your Personal Information at your request, and with your consent, for use by third parties to verify your identity or group eligibility, or as required for the prevention of fraud or otherwise permitted by law.

ID.me may collect Biometric Information from some users as required by the National Institute of Standards and Technology verification standards. Some ID.me partners, such as the IRS and certain state agencies, may require ID.me to verify the identity of an individual to a higher level of certainty as required by the National Institute of Standards and Technology (NIST) guidelines. For additional information regarding what Biometric Information we collect, and how this information may be used, please see our Biometric Information Privacy Policy.

13. Changes to Our Privacy Policy

This Privacy Policy may be periodically updated. This Privacy Policy may be updated periodically to reflect new ID.me features or changes in our Personal Information practices. We will post a notice for consumers at the top of this Privacy Policy of any significant changes. We will indicate at the top of the Privacy Policy when the policy was most recently updated.

14. ID.me Rx

ID.me, including ID.me Rx, will not sell, rent, or trade your Personal Information. ID.me will only transfer your Personal Information at your request, and with your consent, for use by third parties to verify your identity or group eligibility, or as required for the prevention of fraud or otherwise permitted by law.

Use of this Service requires the creation of an ID.me Rx Account. To understand more about ID.me Rx, please review the ID.me Rx Terms of Service. Through your use of ID.me Rx, you consent to ID.me collecting your health information and you understand that ID.me Rx is not subject to the Health Insurance Portability and Accountability Act (HIPAA) when it collects and processes this information.

Information collected through ID.me Rx. We may collect information from or about you in several ways through your use of ID.me Rx and other ID.me Services, including when you choose to share information with us by entering it through our Services, through the postings that you may make, through healthcare providers, through data partners and ID.me Rx Plan Administrators, through your pharmaceutical purchases when using the Services, through pharmacy benefit managers, and by using automated processes. Information collected may include health information about you relating to your use of ID.me Rx, such as the details about prescriptions pricing and discounts obtained, the prescribing physician, the location of the pharmacy at which a prescription is purchased, and details about how you use and interact with ID.me Rx. ID.me Rx may also collect aggregate and de-identified data about the prescriptions purchased across the ID.me Rx platform, this information will not be associated with your ID.me Rx account.

We may use information to provide you with our ID.me Rx Services. We may use the information collected from or about you to provide you with the services requested, to facilitate your obtaining discount pricing on prescriptions, and to provide information that may be of interest to you, such as information about related ID.me Services, newsletters, and special offers. We may also use the information that we collect to customize your experience on our Services, to provide customer support, and to enforce the ID.me Rx Terms of Service.

We may share information with third parties who perform services on our behalf. We may share your information with unaffiliated companies or individuals we hire or work with that provide us with professional advice, business support, or perform services on our behalf, including customer support, web hosting, information technology, payment processing, direct mail and email distribution, and administration, and analytics services. These Service Providers are allowed to use your information to help us provide our Services and not for any other purpose. When using ID.me Rx, you will share, directly with your pharmacy or other third-parties at your discretion, your ID.me Rx Card details in order to obtain applicable discounts. The information you share in your use of ID.me Rx will be subject to the applicable policies and terms provided by those third-parties.

Close your ID.me Rx Account. You may close your ID.me Rx account at any time. By choosing to close your ID.me Rx account, you are directing ID.me to deactivate your ID.me Rx Member ID and to de-identify the data stored in ID.me Rx relating to your use of the Services. Closing your ID.me Rx account does not require the closure of your ID.me account. To the extent that you shared your ID.me Rx Card details with a pharmacy or third-party and they were integrated into your profile and/or account with that third-party, you are responsible for updating and removing any ID.me Rx Card information with such third-party.

15. Contact Us

Whether you're a new or loyal customer, marketer, publisher, media member or job seeker we'd like to stay connected and want to hear from you!

Corporate Address.

ID.me, Inc. 8280 Greensboro Drive, Suite 800 McLean, VA 22102

For Users and Customers.

Member Service Inquiries may be directed to help@id.me.

For Legal Notices.

Legal notices may be directed to legal@id.me.

Copyright © 2022 ID.me, Inc. All rights reserved.