Privacy Impact Assessment for the VA IT System called:

Abbott FreeStyle LibreView-Enterprise

Office of the Chief Health Technology Officer

VA Central Office (VACO)

Date PIA submitted for review:

12/15/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Randall E. Smith	Information System Security Officer (ISSO)	Randall E. Smith
Information System Owner	Scottie Ross	Information System Owner	Scottie Ross

Abstract

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

LibreView is a free cloud-based diabetes management system intended for use by patients, caregivers and healthcare professionals to assist people with diabetes. LibreView supports the VHA Mission of providing exceptional heath care that improves Veterans and qualified family members health and wellbeing by streamlining the care of Veterans with Type 1 or Type 2 Diabetes. Veterans and qualified family members as well as VA healthcare professionals' benefit from statistical historical information provided in clear, intuitive reports that make it easier and faster to discover patterns and trends. LibreView supports Abbott CGM and BGM devices as well as competitor BGMs.

The LibreViewGov SaaS offering enables both healthcare professionals (HCPs) and patients to upload, view, and track glucose measurement readings. Once uploaded, the glucose data is transmitted to the LibreViewGov web application, where the LibreViewGov SaaS generates and presents reports that are viewable by the patient and any HCP or HCP Practice that the patient has connected their account with.

The accreditation boundary for the LibreView SaaS service includes applications and components that reside on Amazon Web Services (AWS) Infrastructure-as-a-Service (IaaS) in the AWS GovCloud USEast region. The LibreView service inherits IaaS security controls from the AWS FedRAMP package for AWS GovCloud, which are documented in the AWS GovCloud FedRAMP System Security Plan.

The LibreView production environment in AWS GovCloud US-East is made of virtual servers (EC2 instances) with Newyu-managed guest OS, Docker containers, Amazon Elastic Container Service (ECS) nodes, applications, Microsoft SQL databases, and tools on Elastic Block Store (EBS) volumes attached to the instances. The production environment also includes several AWS managed services for storage, caching, security, and administration such as Amazon Simple Storage Service (S3), Identity and Access Management (IAM), Glacier, CloudWatch, and CloudTrail.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Abbott FreeStyle LibreView – Enterprise - Enterprise Program Management Office (EPMO)

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

Vendor Owned and non-VA Operated IS. The LibreViewGov SaaS offering enables both healthcare professionals (HCPs) and patients to upload, view, and track glucose measurement readings.

C. Indicate the ownership or control of the IT system or project.

Enterprise Program Management Office (EPMO)

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
1000

E. A general description of the information in the IT system and the purpose for collecting this information.

LibreView is a free cloud-based diabetes management system intended for use by VA patients, caregivers, and healthcare professionals to assist people with diabetes. LibreView supports the VHA Mission of providing exceptional heath care that improves Veterans and qualified family members health and wellbeing by streamlining the care of Veterans with Type 1 or Type 2 Diabetes. Veterans and qualified family members as well as VA healthcare professionals' benefit from statistical historical information provided in clear, intuitive reports that make it easier and faster to discover patterns and trends. LibreView supports Abbott CGM and BGM devices as well as competitor BGMs.

The LibreViewGov SaaS offering enables both healthcare professionals (HCPs) and patients to upload, view, and track glucose measurement readings. Once uploaded, the glucose data is transmitted to the LibreViewGov web application, where the LibreViewGov SaaS generates and presents reports that are viewable by the patient and any HCP or HCP Practice that the patient has connected their account with.

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

The LibreViewGov production environment in AWS GovCloud US-East is made of virtual servers (EC2 instances) with Newyu-managed guest OS, Docker containers, Amazon Elastic Container Service (ECS) nodes, applications, Microsoft SQL databases, and tools on Elastic Block Store (EBS) volumes attached to the instances. The production environment also includes several AWS managed services for storage, caching, security, and administration such as Amazon Simple Storage Service (S3), Amazon Simple Notification Service (SNS), Identity and Access Management (IAM), Glacier, CloudWatch, and CloudTrail.

G. 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.

LibreViewGov is a Vendor Owned and non-VA Operated SaaS product- Amazon Web Services GovCloud (US) Moderate

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

Abbott FreeStyle LibreView - Enterprise #1118 24VA10A7 Patient Medical Records-VA. The retention schedule applicable to LibreView is GRS 5.2 Transitory and Intermediary Records https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

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

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
N/A

K. *Whether the completion of this PIA could potentially result in technology changes*
N/A

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

For Patient accounts, Name (FN, MI, LN), Date of Birth and Email are collected. For HCPs/Clinicians, Name (FN, LN), Email, Work Phone, and Work Address are collected.

In addition to the PII data, PHI is collected for Patients, PHI collected includes Blood Glucose measurement data from continuous glucose meters and blood glucose meters.

PII Mapping of Components (Servers/Database)

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

LibreView is a Cloud Service as a Software (SaaS) consisting of vendor owned virtual servers, VA does not host on premises key components or virtual servers/databases. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by LibreView and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

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

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

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

Patients and HCPs ("End Users"), and the system provide data for diabetes management purposes. Data includes information collected as part of account creation or modification and health data transmitted from a glucose device. HCPs may also manually note.

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

LibreView processes the health data and generates a detailed, consistent set of clear, intuitive reports that make it easier and faster to discover patterns and trends in the patient's management of Diabetes.

Reports are accessible only by the Patients or HCPs after authentication and authorization to LibreView.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

PHI collected includes Blood Glucose measurement data from continuous glucose meters and blood glucose meters

1.3 How is the information collected?

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

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

Patients and HCPs ("End Users") enter data directly through the LibreView website when creating an account or modifying account information. HCPs may also manually enter notes. Health data is transmitted automatically from the glucose device when connected by the end user. Data is transmitted and stored encrypted in government approved cloud services.

1.3b 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.

N/A

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

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

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

Both Patient and HCP user types have the ability to verify and self-service corrections to their account information as needed. Patients and HCPs can also identity inaccuracies and report through a support ticket to the LibreView Support Staff for resolution/correction.

1.4b 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.

There is no contract and no need for one given this is a free service offering for users of the Abbott hardware. VHA prescribes Abbott hardware to veterans so veterans and their providers can use the platform for $0 to VHA.

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 collection, processing, and dissemination of health information must follow the rules and regulations established by the:

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

The LibreView terms and conditions to be read and acknowledged by the Veteran in registering for LibreView, contains a Privacy Act "Routine Uses" section describing how the information will be used. Additionally, the collection, processing, and dissemination of LibreView must follow the rules and regulations established by the:

Title 38 United States Code (U.S.C.), Section 111

Title 38 Code of Federal Regulations (CFR) Sections 70.1, 70.2, 70.3, 70.4, 70.10, 70.20, 70.21, 70.30, 70.31, 70.32, 70.40, 70.41, 70.42, 70.50

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

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

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

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

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

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

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

Privacy Risk: The system collects, processes, and retains PII and PHI on Veterans. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

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.

Data collected; Name and Date of Birth, (DOB) – patient communication with LibreView Used to identify patient age and confirm patient identity Health Insurance Beneficiary Account Numbers: Used to communicate and bill third party health care plans.

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

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

reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

LibreView uses standard statistical analysis to present the inputted data in graphical format for review by end users as part of a diabetes management program. End users may tailor reports to limit the data shown by glucose device and/or time period.

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

LibreView does not make any information available to the users of the system that is not already available in the Electronic Health Record (VistA).

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

The LibreViewGov system will provide the ability, in coordination with Federal government customer tenants, to route all customer data through a dedicated logical or physical network connection. 2. The LibreViewGov system must exclude co-tenant data, or any other third-party data, not intended for the government from being transmitted through a government network connection. 3. The service shall be capable of excluding data intended solely for government use from being routed through an external (non-dedicated) network connection. Interface: https://www.okta.com/ Organization: Okta Connection Security: HTTPS/TLS 1.2 Data direction: Incoming and outgoing Data type for transmission: Internal administrator identity federation Port: 443 Interface: https://www.mailgun.com/ Organization: Mail gun Connection Security: HTTPS/TLS 1.2 Data direction: Outgoing Data type for transmission: Email notifications Port: 443 Customer data is encrypted using full-disk encryption via KMS on the EBS volumes which uses FIPS-compliant AES-256.

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

N/A

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

Customer data backed up to S3 buckets are encrypted using KMS server-side encryption which uses FIPS-compliant AES-256. Newyu Responsibility Symmetric encryption is used by several AWS services, including S3 and EBS volume encryption, which Newyu employs to encrypt customer data

at rest. With Amazon EBS encryption using AWS KMS, any customer data ingested is encrypted using whole volume encryption. AWS Responsibility This control is partially inherited from AWS. AWS establishes and manages cryptographic keys employed within the AWS services such as EBS-volume encryption and S3 server-side encryption in accordance with Federally approved and validated cryptography requirements for key generation, distribution, storage, access, and destruction.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

The PII information collected is the minimal necessary to support the business requirements for the system and is relevant to the mission and needs of the project. The information that is collected is only utilized by the Patients and HCPs ("End Users") and is not shared with external systems.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

For the cloud system, access control includes VA and CSP responsibilities. Newyu, the CSP, follows a formal documented process in accordance with FedRAMP mandated NIST controls for Access Control Access is only provided to the production environment through a formal Access Control request process which includes ensuring thorough evaluation of the requested access and role and only provided with CEO approval and verification of necessary training completion. Access to the community government cloud instance of LibreViewGov SaaS is limited to a subset of the SecOps and DevOps team (expected to be less than 6). All access to PII or PHI data is audited, and is access logged in the Security Information and Event Management (SIEM). All accounts with production access are reviewed monthly with management and senior leadership in ISMS meetings. All production access is terminated within 15 minutes of an employee with production access leaving the company. All flow of information within LibreView is carefully controlled and protected.

2.4c Does access require manager approval?

Access is also patient managed, meaning the patient grants access to all individuals who they will allow to view their data.

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

All access to PII or PHI data is audited, and is access logged in the Security Information and Event Management (SIEM).

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

All accounts with production access are reviewed monthly with management and senior leadership in ISMS meetings. All production access is terminated within 15 minutes of an employee with production access leaving the company. All flow of information within LibreView is carefully controlled and protected.

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*

All information described in Question 1.1* is retained by the system until the account owner (end user) deletes the relevant account(s), or unless otherwise indicated by the VA. LibreViewGov is not a system of record but a supporting system not subject to data retention policies. All data contained herein relevant to clinical care is present in the system of record and will follow VA/VHA data retention policies as appropriate. *Name (patient/clinician), DOB (patient), personal email (patient), LibreView unique ID (patient/clinician), Blood Glucose measurement data (patient), Work email (clinician), Work phone (clinician), Work address (clinician)

3.2 How long is information retained?

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

early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

All information described in Question 1.1 is retained by the system until the account owner (end user) deletes the relevant account(s)

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

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

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

LibreViewGov does not own the information. The end user owns all the information, and they determine when they want to delete it.

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

The retention schedule applicable to LibreView is GRS 5.2 Transitory and Intermediary Records https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

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

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

When an account is removed the relevant data is deleted from the database system of the SaaS within 24 hours through an automated process.

VA Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then

permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

Identifiable data is not used for research, testing or training. Newyu Symmetric encryption maintains strict access controls to ensure data is not accessed without permission.

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

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

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

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

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

Follow the format below:

Privacy Risk: There is always a chance that the end user may never delete their account.

Mitigation: HCPs may remove inactive patient accounts from their view at any time. Removed patients will still have access and control of their own accounts but their data would no longer be shared with VA staff.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

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

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

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

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

Follow the format below:

Privacy Risk: There is no information shared from this system.

Mitigation: There is no information shared from this system.

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	***List the purpose of information being***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding***	***List the method of transmission and the***

shared/received with	***shared / received / transmitted with the specified program office or IT system***		***agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***measures in place to secure data***
N/A	N/A	N/A	N/A	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: There is no information shared from this system.

Mitigation: There is no information shared from this system.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also

provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

A flash page consent is reviewed and acknowledged by End users accepting a privacy notice at account creation and each time the notice is modified. The notice is attached in Appendix A.

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

N/A

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

A consent is reviewed and acknowledged by End users accepting a privacy notice at account creation and each time the notice is modified. The notice is attached in Appendix A.
LIBREVIEW PATIENT/INDIVIDUAL USER TERMS OF USE PRIVACY NOTICE (libreview.com), PRIVACY NOTICE (libreview.com), LIBREVIEW PROFESSIONAL TERMS OF USE

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.

Patients may elect not to share data with their HCP(s) in their account settings. Additionally, a patient may elect to remove access from their HCP(s) in their account settings. LibreView is a secondary viewer – the original data resides on the glucose device. If a patient does not wish to provide access from within LibreView, they are able to bring their glucose device directly to their HCP(s) to review.

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.

Consent is provided for use of the website as a whole although sharing data is controlled as above. The notice is attached in Appendix A.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is always the risk that the user may not read the Notice when signing into the account.

Mitigation: The user is required to agree to the terms before they can move forward with entering their information.

Section 7. Access, Redress, and Correction

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

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

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

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

The patient has total control of the data and is able to correct erroneous information (an example would be a data reading being removed from view, which is grossly off pointing to equipment or material failure) to ensure statistical models can be utilized sensibly. Medical staff are limited to view-only access to the data, with the patient's explicit permission.

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

N/A

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

N/A

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.

Patients and HCPs ("End Users") are able to review and correct inaccurate or erroneous information through self-service within LibreView. An escalation or support process is also provided where an End User can contact and open a ticket for support in correcting inaccurate or erroneous information.

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.

Self Service of PII is available in the Account Settings option of the LibreView software in the main menu. Additionally, a link to the Support system which allows End Users to contact customer support is also available in the main menu of LibreView.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or

group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Patients and HCPs ("End Users") may directly access and correct or update their information online.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: The privacy risk of this system lies in the possibility of VA clinicians inputting notes or responding to patient-initiated notes with PII, PHI, or patient-care data and not putting pertinent information in the health record.

Mitigation: Clinicians are trained and expected to not to include any sensitive data in the notes. Patient-care decisions and VA records are to be kept in the EMR/EHR.

Section 8. Technical Access and Security

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

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

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

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

LibreView consists of the following roles: 1. HCP Practice Administrator 2. HCP 3. Patient

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

LIBREVIEW PROFESSIONAL TERMS OF USE
LIBREVIEW PATIENT/INDIVIDUAL USER TERMS OF USE

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

An HCP with access to LibreView may create a Practice and invite other HCPs to participate in the practice. The Practice creator is always the HCP Practice Administrator. The HCP Practice Administrator may make any other HCP in the practice an Administrator or remove access from another administrator. An HCP may send an invite to a Patient through an email. A patient that accepts the invite will self- register an account but automatically be placed in the HCP's practice (a patient may remove themselves from a practice at any time). Additionally, an HCP may create a patient account on behalf of the patient. This account will not have an associated logon capability and will only receive updated data when the patient visits the HCP's practice. HCP Practice Administrators are able to invite or remove HCPs from the practice. All HCPs within a practice can view the patients of the practice. An HCP who has been removed from a practice will no longer have access to those patients. An HCP may upload blood glucose data from a device on behalf of a patient, generate a report for a patient and invite an existing patient to the practice. Patients have the ability to upload blood glucose data, control which practices have access to their data and may generate reports. No other users from any other agencies have access to the system. PII is only shared within the practice.

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.

LibreView is an external SaaS developed and managed by Newyu, Inc. Newyu does employ contractors for both design and maintenance. NDA and Rules of Behavior are developed for contractors who work on the system and are available for review. Newyu, Inc. - LibreView for US

Government Package ID FR2000174962 is an FEDRAMP Approved SaaS
https://marketplace.fedramp.gov/#!/product/libreview-for-us-government?sort=productName
Trademarks are the property of their respective owners.

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 VHA staff are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training. In addition, all employees who have access to patient health information must also completed the Privacy and HIPAA Focused training. These trainings are available on the Talent Management Systems.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 14-Mar-2022
3. *The Authorization Status:* Authorize to Operate
4. *The Authorization Date:* 12-Mar-2020
5. *The Authorization Termination Date:* 13 Mar 2023
6. *The Risk Review Completion Date:* 28-Sep-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.

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

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include:

Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

LibreViewGov is a SaaS product - Amazon Web Services GovCloud (US) Moderate

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

N/A

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.01.20 15:09:15 -05'00'

Privacy Officer, Abbott FreeStyle LibreView-Enterprise

RANDALL SMITH

Digitally signed by RANDALL SMITH
Date: 2023.01.20 13:31:57 -06'00'

Information Systems Security Officer, Randall E. Smith

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2023.01.23 19:19:48 -05'00'

Information Systems Owner, Scottie Ross

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

LIBREVIEW PATIENT/INDIVIDUAL USER TERMS OF USE PRIVACY NOTICE (libreview.com), PRIVACY NOTICE (libreview.com), LIBREVIEW PROFESSIONAL TERMS OF USE.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices