Privacy Impact Assessment for the VA IT System called:

LoanerLink

Veterans' Health Administration (VHA)

Enterprise Operations

Date PIA submitted for review:

February 14, 2023

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)	William Eric Roberts	william.roberts@va.gov	614.257.5981
Information System Owner	Steven J. Gaj	steven.gaj@va.gov	216.701.0647

Abstract

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

Censis Technology Inc.'s LoanerLink applications is a cloud-based, Software-as-a-Service (SaaS) application that provides the Sterile Processing Department (SPD) the flexibility to manage their facility's equipment loaner process. Access to LoanerLink is restricted by requiring use of Censis created accounts implementing username/password authentication. LoanerLink does not interconnect with or share data with other vender systems. LoanerLink dataset is as follows: Name of surgeon, Business Email Address, Business Phone Number, Case Code, Trays, Procedure, Date/Time of Procedure, Operating Room Location, Date/Time of Procedure, Date/Time of Loaner tray delivery or pickup, Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor Phone (Text).

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.

The IT System name is LoanerLink®. The program office that owns the IT system is Office of Information Technology (OIT).

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

The application helps hospitals manage communication flow and loaner assets with vendor representatives. It provides confirmation of scheduled surgeries and provides a means of constant communication flow between hospital and vendor. Communication can include email, text or phone. End state: Timely delivery of loaner trays so they can be sterilized in accordance with the facility Standard Operating Procedure (SOP) before surgery and then picked up from the facility in a timely manner.

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

Veteran's Health Administration, Enterprise Operations

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.

Currently Cincinnati VAMC has 6 months of data, approximately 350 cases. The vendor expects to implement this application at approximately 39 VA Medical Centers and the expected number of

annual cases is 13,650. VA SPD employees and their assigned vendors will utilize the application to manage the surgical equipment loaner trays.
Data Set:
- Name of Surgeon, Business Email Address, Business Phone Number, Case Code.
- Trays, Procedure, Date/Time of Procedure, Operating Room Location, Date/Time of Loaner tray delivery or pickup.
- Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor Phone (Text).

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

Censis Technology Inc.'s LoanerLink applications is a cloud-based, Software-as-a-Service (SaaS) application that provides the Sterile Processing Department (SPD) the flexibility to manage their facility's equipment loaner process. Access to LoanerLink is restricted by requiring use of Censis created accounts implementing username/password authentication. LoanerLink does not interconnect with or share data with other vender systems. LoanerLink dataset is as follows: Name of surgeon, Business Email Address, Business Phone Number, Case Code, Trays, Procedure, Date/Time of Procedure, Operating Room Location, Date/Time of Procedure, Date/Time of Loaner tray delivery or pickup, Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor Phone (Text).

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

Not Applicable

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.

This system is operated in more than one site. The same controls are used across all sites. PII is maintained consistently as there is only a single repository of all data.

3. Legal Authority and SORN

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

This system is operated in more than one site. The same controls are used across all sites. PII is maintained consistently as there is only a single repository of all data.

SORN: Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10).
AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

LoanerLink System operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration - Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by
the:
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

79VA10 Veterans Health Information Systems and technology Architecture (VISTA) Records-VA. 79VA10 / 85 FR 84 which provides the following authority: AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

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?*
Not Applicable

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
Not Applicable

K. *Whether the completion of this PIA could potentially result in technology changes*
Not Applicable

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)

Data Set:

- Name of Surgeon, Business Email Address, Business Phone Number, Case Code.
- Trays, Procedure, Date/Time of Procedure, Operating Room Location, Date/Time of Loaner tray delivery or pickup.
- Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor Phone (Text).

PII Mapping of Components (Servers/Database)

LoanerLink consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by LoanerLink 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
Production – Web Server	Yes – Collect	No	VA Employee/Contractor Name & Email Address	Used for Authentication and Notification Emails	HTTPS & TLS Secure Website requiring authentication
Production – Database Server	Yes - Store	Yes	VA Employee/Contractor Name & Email Address	Used for Authentication and Notification Emails	Restricted-Access Database in Private Cloud

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?

Information is added to the system by VA Employees having LoanerLink Account Administration Rights. Additionally, pickup/delivery status is added to the system by VA business partners providing loaner sterilization trays.

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.

Not Applicable

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

The system creates delivery/pickup status reports.

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?

Information is added to the system by VA Employees having LoanerLink Account Administration Rights. Additionally, pickup/delivery status is added to the system by VA business partners providing loaner sterilization trays.

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.

Not Applicable

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.

Information input directly from system users be assumed to be accurate.. Additionally, account holders observe and test the accuracy of information when they access LoanerLink or are provided notifications of loaner tray delivery/pickup status.

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.

Information input directly from system users be assumed to be accurate.. Additionally, account holders observe and test the accuracy of information when they access LoanerLink or are provided notifications of loaner tray delivery/pickup status.

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

LoanerLink System operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration - Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by
the:
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

79VA10 Veterans Health Information Systems and technology Architecture (VISTA) Records-VA. 79VA10 / 85 FR 84 which provides the following authority: AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

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. (*Work with your System ISSO to complete this section)*

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: LoanerLink contains Personally Identifiable Information (PII) limited to VA and Business Partner Name and email address. The disclosure of VA employee name (physician name) and government email is low privacy risk as this information is commonly available on the VA Facility public-facing websites.

Mitigation: There are multiple controls in place to mitigate privacy violations. These controls are technical, physical and administrative in nature. LoanerLink Information System is protected with data encryption at rest and during transmission. LoanerLink is hosted in a Secure Data Warehouse; LoanerLink system uses a current supported and managed operating system and hosted behind both a Firewall and Intrusion Detection System (IDS). All users of LoanerLink are mandated to complete Information Security and Privacy/HIPAA training on an annual basis.

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 application helps hospitals manage communication flow and loaner assets with vendor representatives. It provides confirmation of scheduled surgeries and provides a means of constant communication flow between hospital and vendor. Communication can include email, text or phone. End state: Timely delivery of loaner trays so they can be sterilized in accordance with facility SOPs before surgery and then picked up from the facility in a timely manner.
This IT system collects, uses, disseminates creates and maintains the following information:
Name of Surgeon- Used to identify the physician associated with the procedure loaner tray in the loaner tray status notification emails.

Business Email Address – Used for status notification communication.
Business Phone Number – Used for notification communication
Case Code – Used by VA staff to correlate loaner tray to patient
Procedure – Used to correlate loaner try to specific procedure
Trays – Identification of trays used in the Procedure
Date/Time of Procedure – Used for scheduling loaner tray
Operating Room Location – Used for facilitating loaner tray drop off
Date/Time of Loaner tray delivery or pickup – used for loaner tray status
Contractor's Name – Vendor's Name
Contractor's Email – Confirmation of scheduled surgeries and provides communication flow between hospital and vendor.
Contractor's Phone Number – Confirmation of scheduled surgeries and provides communication flow between hospital and vendor.
Contractor Phone (Text) – Confirmation of scheduled surgeries and provides communication flow between hospital and vendor.

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.

Analysis of data and reporting is limited to pickup/delivery status notifications of loaner sterilization trays for procedures.

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.

Analysis of data and reporting is limited to pickup/delivery status notifications of loaner sterilization trays for procedures.

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?

HTTPS & TLS Secure Website requiring authentication, Restricted-Access Database in Private Cloud.

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

HTTPS & TLS Secure Website requiring authentication, Restricted-Access Database in Private Cloud.

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

HTTPS & TLS Secure Website requiring authentication, Restricted-Access Database in Private Cloud.

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 requirement for access to LoanerLink PII is determined by Sterilization/Surgery Service Chiefs based on the Facility's participation in LoanerLink and requirement to receive sterilization loaner tray notifications to facilitate the delivery of healthcare.

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

Access to LoanerLink is granted and ongoing account management is conducted referencing the LoanerLink Access Control SOP utilizing the VA Light Electronic Action Framework (LEAF). LEAF is a System of Record.

2.4c Does access require manager approval?

Service Chief and Area Manager Control approval are required within VA Light Electronic Action Framework (LEAF) at each facility utilizing LoanerLink.

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

VA LoanerLink Administrators at each participating facility will create the accounts for the LoanerLink user with approved access upon receiving a LEAF approval notification.

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

Both VA and Censis supervisors are responsible for supervising the use of LoanerLink PII.

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*

LoanerLink retains the identified Data Set:
- Name of Surgeon, Business Email Address, Business Phone Number, Case Code.
- Trays, Procedure, Date/Time of Procedure, Operating Room Location, Date/Time of Loaner tray delivery or pickup.
- Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor Phone (Text).

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.*

Records Control Schedule 10-1 (va.gov)

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years

after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

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?

LoanerLink operates using 2 NARA approved retention schedules:
• Department of Veterans Affairs, Veterans Health Administration Records Control Schedule 10-1 November 2017) https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
• Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31). Records Control Schedule 10-1 (va.gov)

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.

At the end of the retention period data is deleted/purge electronically from the LoanerLink Database.

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.

Non-Applicable. LoanerLink does not provide information 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. (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: The PII information retained is subject to breach, loss and destruction from external, internal and physical risks.

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, planning and maintenance.

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?

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

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

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

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

Data Shared with Internal Organizations

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

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Mitigation: Non-Applicable

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.

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***

LoanerLink – Software as a Service (SaaS)	Sterilization Tray scheduling and notifications for delivery/pickup	Name of Surgeon, Business Email Address, Business Phone Number, Case Code, Trays, Procedure, Data/Time of Procedure, Operating Room Location, Date/Time of Loaner tray delivery or pickup, Contractor's Name, Contractor's Company Email, Contractor's Phone Number, Contractor's Phone Number (Text).	MOU ISA; VA Authority to Operate (ATO)	HTTPS & TLS FIPS 140-2 encryption

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 a risk that the information could be shared with an external organization or agency that does not have a legal authority to access VA data. The information could be redisclosed by the external organization or agency.

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, planning and maintenance.

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.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." Notice is also provided in the Federal Register with the publication of the SORN: Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10

Employees and VA contractors are required to provide the requested information to maintain employment or their contract with the VA.
Notice is provided through the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online.

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

Not Applicable
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.

Employees and VA contractors are required to provide the requested information to maintain employment or their contract with the VA.
Notice is provided through the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online.

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.

Employees and VA contractors are required to provide the requested information to maintain employment or their contract with the VA.

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.

Not Applicable. The use of PII information by LoanerLink is narrow and specific to the business purpose of delivery and pickup status for sterilization loaner trays for the delivery of healthcare – LoanerLink PII is not used nor authorized for any other purpose.

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 a risk that an individual VA Employee may not receive notice that their name is being collected, maintained, processed, or disseminated by the Veterans' Health Administration.

Mitigation: Mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

Privacy Risk: There is a risk that an individual VA Employee PII is being collected, maintained, processed, or disseminated by the Veterans' Health Administration in a manner not authorized by the VA employee.

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.***

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

Access and redress is specified in the SORN 79VA10 Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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).

Not Applicable

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.

Not Applicable

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.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

Access and redress is specified in the SORN 79VA10 Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact

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.

.

Access and redress is specified in the SORN 79VA10 Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact

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.

Redress is provided through the Privacy Act for the individual to view and request correction to the inaccurate or erroneous information. If the request is denied, the individual is advised of his/her right to appeal the decision by writing to the Office of General Counsel (024); Department of Veteran Affairs; 810 N.W.; Washington, D.C. 20420.
The Privacy Act and HIPAA permit the individual to also complete a Statement of Disagreement to the information that was denied correction. The facility may include a rebuttal to the Statement of Disagreement. The Statement of Disagreement, rebuttal, and denial letter are attached to the information at any time the information is authorized for release

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: There is a risk that an employee or contractor may not know how to request corrections to their PII for LoanerLink.

Mitigation: Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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.

The requirement for access to LoanerLink PII is determined by Sterilization/Surgery Service Chiefs based on the Facility's participation in LoanerLink and requirement to receive sterilization loaner tray notifications to facilitate the delivery of healthcare.

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?

Access to LoanerLink is granted and ongoing account management is conducted referencing the LoanerLink Access Control SOP utilizing the VA Light Electronic Action Framework (LEAF). LEAF is a System of Record

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.

Service Chief and Area Manager Control approval are required within LEAF at each facility utilizing LoanerLink. VA LoanerLink Administrators at each participating facility will create the accounts for the LoanerLink user with approved access upon receiving a LEAF approval notification. Both VA and Censis supervisors are responsible for supervising the use of LoanerLink PII.

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.

There is a BAA between the VA and Censis Technologies. LoanerLink is Software as a Service and is owned and maintained by Censis Technologies.
There is an existing contract in place for facilities using LoanerLink. Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee which includes the facility Privacy Officer and Information Security Officer and Chief Information Officer). This review is conducted each time the contract period expires. Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

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 users accessing the Veterans Administration (VA) Network and Information Systems are required to complete initial annual VA Privacy and Information Security Awareness and Rules of Behavior training or Mandatory Training for Trainees (MTT), VA Privacy & HIPAA Awareness training, and/or equivalent training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* 05/09/22
2. *The System Security Plan Status Date:* 05/09/22
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 02/02/23
5. *The Authorization Termination Date:* 02/02/25
6. *The Risk Review Completion Date:* 02/02/23
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.***

Not Applicable

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.

LoanerLink is in the AWS public cloud, which is FedRAMP. LoanerLink itself is not FedRAMP as it will have its own instance; therefore, according to PSF Team it doesn't need to be FedRAMP. LoanerLink does have a VA Authority to Operate (ATO).

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.*

A Business Associate Agreement (BAA) defines responsibilities. A Memorandum of Understanding / Interconnection Security Agreement (MOU ISA) defines the data as VA Owned Moderate data and the responsibilities to protect the data. VA Contract Security clauses define these responsibilities.

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.

Not Applicable

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.

A Business Associate Agreement (BAA) defines responsibilities. A Memorandum of Understanding / Interconnection Security Agreement (MOU ISA) defines the data as VA Owned Moderate data and the responsibilities to protect the data. VA Contract Security clauses define these responsibilities.

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).

Not Applicable

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.03.21 12:49:35 -04'00'

Privacy Officer, Nancy Katz-Johnson

William E Roberts 1143984

Digitally signed by William E Roberts 1143984
Date: 2023.03.21 12:45:57 -04'00'

Information System Security Officer, William Eric Roberts

2023.03.21 13:15:54 -04'00'

Information System Owner, Steven J. Gaj

APPENDIX A-6.1

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

https://www.oprm.va.gov/docs/Privacy_Act_Systems_of_Records.xls

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