Privacy Impact Assessment for the NON-VA IT System called:

Life Image Cloud

Office of Electronic Health Record Modernization (OEHRM)

Date PIA submitted for review:

April 9, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Raymond Walters	Raymond.Walters@va.gov	906-774-3300 Ext. 32025
Information System Owner	Michael Hartzell	Michael.Hartzell@va.gov	803-406-0112

Abstract

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

Life Image Cloud is a secure gateway enabling bi-directional imaging and medical data interoperability between VA Medical Centers (VAMC's) and Community Care Network (CCN) Providers, supporting the implementation of the VA Maintaining Internal Systems and Strengthening Integrated Outside Networks Act of 2018, a.k.a. the MISSION Act, which gives Veterans greater access to health care in VA facilities and the community, expands benefits for caregivers, and improves VA's ability to recruit and retain the best medical providers.

Overview

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

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

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

Life Image Cloud is a Non-VA system that augments the VA/DoD Joint Electronic Health Record (JEHR) system. Life Image Cloud functions as a secure gateway enabling bi-directional imaging and medical data interoperability between VA Medical Centers (VAMC's) and Community Care Network (CCN) Providers. The backbone of this technology is Life Image Transfer Exchange (LITE) software designed specifically to meet stringent security and regulatory protocols to support implementation of the VA Maintaining Internal Systems and Strengthening Integrated Outside Networks Act of 2018, a.k.a. the MISSION Act, which gives Veterans greater access to health care in VA facilities and the community, expands benefits for caregivers, and improves VA's ability to recruit and retain the best medical providers. Version 2.3.54 of LITE was approved by the VA Technical Reference Model (TRM) Management Group on 28 October 2020.

Life Image Cloud is planned for deployment in alignment with the Office of Electronic Heath Record Modernization (OEHRM) Capability Set 2.0. Life Image Cloud resides in Google Gov-Cloud, a FedRAMP authorized Infrastructure as a Service (IaaS) cloud solution. Life Image Cloud, however, has not been assessed as a Cloud Service Provider (CSP) solution. Life Image Inc. is a contractor of Cerner Corp., a Subcontractor/Business Associates of OEHRM. Life Image Inc. does not directly have a contract with OEHRM. The Veterans Health Administration (VHA) remains the owner of VHA data being shared via Life Image Cloud. In the role of a Business Associate of the VHA, OEHRM will take responsibility in validation/assessment of security and privacy mechanisms for the VHA patient data held/processed by Life Image Cloud.

By design, Life Image Cloud is used for the senders to stage patient Digital Imaging and Communications in Medicine (DICOM) data within a short period of time until the data packages, or "studies", are picked up/downloaded by the intended receivers, using secured URL and password. The expected number of individuals whose information is stored in the system in a certain period of time can vary from zero to a few hundred packages or studies. Life Image Cloud is an enterprise solution which can support VHA "internal" providers/clinicians in multiple VAMC locations to exchange DICOM data with CCN providers.

As having stated in section 3.2.8, Trusted Behavior Expectations, of the Memorandum of Understanding and Interconnection Security Agreement (MOU-ISA) signed between VA Data Access Services Cloud Single Point of Entry (DAS SPOE) and Life Image Inc. on March 10, 2021, "The Department of Veterans Affairs system and users are expected to protect Life Image Inc., and Life Image Inc.'s system and users are expected to protect the DAS Cloud system in accordance with the Privacy Act and Trade Secret Act (18 U.S.C. 1905), the Unauthorized Access Act (18 U.S.C. 2701 and 2710), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), System of Record Notice (SORN) 24VA10A7 – Patient Medical Records-VA, and other applicable laws and policies referenced in Section 1.1 of the MOU-ISA."

There is no indication that the completion of this PIA will either require changes in business processes or changes of technology. If PII/PHI is disclosed without authorization by Life Image

Cloud, either intentionally or unintentionally, the magnitude of harm would be considered at moderate to low risk level. VA data breach notification and incident response processes would be followed accordingly.

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 Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☒ Other Unique Identifying Number (list below)

All data elements listed above (name, data of birth, address, MRN) and gender data element are integrated in the Digital Imaging and Communications in Medicine (DICOM) data file (or study) being staged in Life Image Cloud.

PII Mapping of Components

Life Image Cloud consists of 1 key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Life Image Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
FRC DB01	Yes	Yes	Patient name, address, Medical Records Number (MRN), date of birth, DICOM data	Interoperability between VAMC's and CCN Providers	Hypertext Transfer Protocol Secure (HTTPS)

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

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

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

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

DICOM data, which includes the radiology, cardiology, dental image(s) and integrated PII elements, can be sent to the Life Image Cloud from either a VAMC or a CCN Provider, depending on the business use case. From the CCN Provider side, a Picture Archiving and Communication System (PACS) Administrator will push selected images to Life Image Cloud, using pre-defined Uniform Resource Locator (URL) and passcode provided by the VA requester. From the VA side, a clinician (Provider) can request image(s) release from CareAware MultiMedia 7 Archive (CAMM 7) database cluster in the Federal Enclave to a selected CCN Provider via Life Image Cloud.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

DICOM data, including the imagery and integrated PII elements, exchanged through Life Image Cloud is not collected directly from patients/individuals. It is pushed/uploaded via secured electronic transmission from either a CCN Provider PACS database or the Joint EHR/Federal Enclave CAMM 7 database cluster.

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

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

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

The purpose of using Life Image Cloud to share Veterans/patients DICOM data (imagery and integrated PII elements) is to support implementation of the VA Maintaining Internal Systems and Strengthening Integrated Outside Networks Act of 2018, a.k.a. the MISSION Act, which gives Veterans greater access to health care in VA facilities and the community, expands benefits for caregivers, and improves VA's ability to recruit and retain the best medical providers.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Life Image Cloud is as a DICOM transport service provider. Since data in transit and data at rest is encrypted, Life Image Cloud does not provide data accuracy check mechanism. By design, the receiving entity is responsible for verifying the integrity of patient DICOM data.

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

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

Life Image Cloud is a Non-VA system that augments the VA/DoD Joint Electronic Health Record (JEHR) system, of which authority to operate is stated in System of Record Notification (SORN) 24VA10A7, Patient Medical Records-VA, and in Title 38, United States Code, Sections 501(b) and 304. The MISSION Act of 2018 is the federal legal platform for Life Image Cloud implementation.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk:
There's a risk that data confidentiality and integrity may be compromised if the cryptography is not strong enough.

Mitigation:
DICOM data is encrypted both in transit and at rest, using FIPS 140-2 validated cryptography.

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.

DICOM data of a specific patient is requested by a provider, either internal VA one or external clinician, for the purpose of timely diagnostic and providing healthcare treatment. Life Image Cloud technology and services address this critical need.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The data that passes through the cloud is scanned for virus/malware.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Risk:
This is not a federal system – risk may emerge if the purpose of data usage is not defined. If an incident or breach occurs, what incident handling process to follow? Data files uploaded to Life Image Cloud maybe accessed by unauthorized user(s).

Mitigation:
The MOU-ISA signed on March 8, 2021 between VA DAS Cloud and Life Image Inc. provides security incident response protocol, configuration change control mechanism. All authorized Life Image personnel are required to complete VHA Privacy/HIPAA training at an annual basis. Life Image Cloud is not a federal system hence there's no SORN created directly for the system. However, SORN 168VA005 Health Information Exchange-VA applicable to VA DAS Cloud does clearly state the use of information. By design, only intended receiver(s) of secure email message can access the secure URL and passcode provided by sender.

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

Patient DICOM data, which includes imagery and PII elements, is transitory and only resides in the cloud for the length of time it takes to traverse to final destination. Once transmission completes data is purged from the system.

3.2 How long is information retained?

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

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

The Life Image software contains a purge job that runs automatically once transmission is complete to the destination.

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

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

Life Image Cloud is a Non-VA system that augments the VA/DoD Joint Electronic Health Record (JEHR) system. By design, DICOM data, in the form of "studies" or "packages" uploaded by the sender, only stages or resides in the system until they are picked up/downloaded by the receiver, using the Uniform Resource Locator (URL) and passcode provided by the sender via secure email. A purge job is run automatically right after transmission is completed. All other system data logs must be in alignment with the record retention schedules applicable to the JHER system, which are

- Records Control Schedule 10-1 (January 2020) https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
- Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

3.4 What are the procedures for the elimination of SPI?

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

By design, DICOM data, in the form of "studies" or "packages" uploaded by the sender, only stages or resides in the system until they are picked up/downloaded by the receiver, using the Uniform Resource Locator (URL) and passcode provided by the sender via secure email. A purge job is run automatically right after transmission is completed.

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

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

Not applicable, Life Image does not use patient data for any of the above-mentioned uses.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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.

Privacy Risk:
N/A – There's no risk identified, with reference to both the Principle of Minimization and Principle of Data Quality and Integrity. The system is designed with FIPS 140-2 encryption compliance hence data in transit and at rest is secured. By design, data is purged immediately after transmission is completed.

Mitigation:
N/A

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Office of Information and Technology (OIT) - VA Enterprise Cloud (VAEC) - Data Access Services – Single Point of Entry (DAS SPOE)	Health care treatment	Patient name, address, Medical Records Number (MRN), date of birth, DICOM data	Hypertext Transfer Protocol Secure (HTTPS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Privacy Risk: N/A – No privacy risk identified with reference to sharing of information within VA/VHA – and extending to the CCN providers. The process is designed by which, the sender will send the intended receiver the URL and passcode via secure email so that the receiver can download the DICOM "study" staged in Life Image Cloud.

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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 data element types such as PII/PHI that are shared/received 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***
CCN Providers – LITE Device	Health care treatment	Patient name, address, Medical Records Number (MRN), date of birth, DICOM data	Contracts with CCN Third Party Administrators (Optum, TriWest)	Hypertext Transfer Protocol Secure (HTTPS)
Cerner Corp - Life Image Local Appliance (LILA)	Health care treatment	Patient name, address, Medical Records Number (MRN), date of birth, DICOM data	Business Associate Agreement (BAA) between Life Image Inc. and Cerner Corp., 4 Nov 2013	HTTPS

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

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

Privacy Risk: N/A - No privacy risk identified with reference to sharing of information outside of the Department – in this case, the system is majorly used for the purpose of sharing patient DICOM data with outside care providers, or CCN providers. The process is designed by which, the sender will send the intended receiver the URL and passcode via secure email so that the receiver can download the DICOM "study" staged in Life Image Cloud.

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Life Image Cloud does not collect PII directly from individuals. Life Image Cloud augments the Joint EHR system, of which SORN 24VA10A7 (2020-21426.pdf (govinfo.gov)– Patient Medical Records-VA was published in Federal Register on October 2, 2020. Notice is provided to individuals through this SORN as well as this PIA.

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

Life Image Cloud collects PII from another system (the Joint EHR system), not directly from individuals hence they do not have the opportunity to decline providing information.

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

Life Image Cloud collects PII from the Joint EHR system, not directly from individuals hence they do not have the opportunity to consent to particular uses of the information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: N/A

Mitigation: N/A

Section 7. Access, Redress, and Correction

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

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

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

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

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

Life Image Cloud collects PII from the Joint EHR system, not directly from individuals. SORN 24VA10A7- Patient Medical Records-VA was published in Federal Register on October 2, 2020. Notice to individuals is provided by means of the SORN publication as well as the publication of this PIA. Individuals can gain access to their information by following the Notice of Privacy Practice procedures provided by Joint EHR system PIA.

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

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

Individuals can correct inaccurate or erroneous information in their record by following the Notice of Privacy Practice procedures provided by Joint EHR system PIA.

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.

Individuals can correct inaccurate or erroneous information in their record by following the Notice of Privacy Practice procedures provided by Joint EHR system PIA.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Individuals can follow the Notice of Privacy Practice provided by Joint EHR system PIA for redress procedure.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: N/A

Mitigation: N/A

Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The only persons with access to the cloud are Authorized Life Image Support personnel. The cloud is not accessible by any person from the VA or the CCN Providers.

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

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

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

The only persons with access to the Life Image Cloud system are authorized Life Image support personnel. No VA personnel has access to the system.

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 Life Image personnel with clearance are required to complete the VHA Privacy/HIPPA training on an annual basis.

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

If Yes, provide:

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

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

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

This document is being submitted in an effort to obtain ATO and as of today this has not been granted. No IOC date is determined. The FIPS 199 Classification is considered Moderate.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.04.28 14:41:23 -04'00'

Privacy Officer, Rita Grewal

Raymond E. Walters 1578937

Digitally signed by Raymond E. Walters 1578937
Date: 2021.05.03 08:21:05 -05'00'

Information System Security Officer, Raymond Walters

Michael J. Hartzell 3487012

Digitally signed by Michael J. Hartzell 3487012
Date: 2021.04.28 10:04:34 -04'00'

Information System Owner, Michael Hartzell