Privacy Impact Assessment for the VA IT System called:

Laerdal Simulation

System-Building 22 Renovation Project 595-15-201
Lebanon VA Medical Center Education Department
Veterans Health Administration

Date PIA submitted for review:

02/04/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Hromco	Tonya.Hromco@va.gov	717-272-6621 ext. 4614
Information System Security Officer (ISSO)	Matthew Schmuck	Matthew.Schmuck@va.gov	717-272-6621 ext. 4454

	Name	E-mail	Phone Number
Information System Owner	Henna Grover	henna.grover@va.gov	412-216-4566

Abstract

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

The full Laerdal simulation suite includes SimMan 3G, SimMan ALS, Nurse Anne Simulator, VitalsBridge, SimCapture Cloud Services, Simulator Mannequins, New IT Closet and AV equipment infrastructure, Intercom System, TVs, computers, cameras, microphones, projectors, and Education Training Days. These are all on-premise devices that will be connected through the local network and will communicate to LLEAP Laptops and SimPad tablets, which will then communicate to cloud storage in SimCapture Cloud via a plugin. The on-premise devices work together to create video recording live streaming that will be accessible to instructors for debriefing the class on performance, and capturing data metrics during trainings such as the mannequins heart rate, breaths, and compression depth…etc. This data would help instructors provide more in-depth quality training.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

Lebanon VAMC is in the process of renovating their Education department with special emphasis on simulation and skills lab for clinicians. Growing from 800 sq. ft, the Simulation Center space is now 2,000 sq. ft to purposefully perform high-risk activities/procedural tasks within a safe environment to improve skills and learn from error thus improving overall healthcare delivery. They are currently using several standalone Laerdal products for training. The full simulation suite would include SimMan 3G, SimMan ALS, Nurse Anne Simulator, VitalsBridge, SimCapture Cloud Services, Simulator Mannequins, New IT Closet and AV equipment infrastructure, Intercom System, TVs, computers, cameras, microphones, projectors, and Education Training Days. These are all on-premise devices that will be connected through the local network and will not communicate directly out to the cloud. They will instead communicate to LLEAP Laptops and SimPad tablets connected through the local network, which will then communicate to cloud storage in SimCapture Cloud via a plugin. The on-premise devices work together to create video recording, live streaming that will be accessible to instructors via VA email/password for debriefing the class on performance, and capturing data metrics during trainings such as the mannequins heart rate, breaths, and compression depth…etc. This data would help instructors provide more in-depth quality training. Access to these recordings can be limited to only Government Furnished Equipment (GFE) connected to the VA network via Single Sign-On internal (SSOi) limitations. Laerdal Medical does not process any sensitive or special data. Laerdal Medical does store student records such as first and last names, emails, and grades. Laerdal Medical does store audio and video records but does not use or create any biometric data from these records. Laerdal Medical's processing of data does include cross-border processing for support and operations services within the United States. The system supports integration with data-streams from multiple clinical training hardware devices that would be connected to the SimCapture Cloud, provides streamlined training for simulation teams, and mass storage capabilities. The system will be controlled by VA but owned and operated by Laerdal. This software will support employment requirements laid out by VHA directives 1177, Cardiopulmonary Resuscitation, and 1101.05(2), Emergency Medicine

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

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

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

- VA Email
- PIV #
- Grades
- Audio/Video Recordings

PII Mapping of Components

SimCapture Cloud consists of 2 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SimCapture Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

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

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

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

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

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

The system uses the clients SSO system for authentication and collects the users name and email to display and identify the user in the software.

The system also collects data from training devices such a simulated heart rates to display with the users training results as these are the devices they are training on.

The system may also generate scores or other reports to display as part of the users' training results.

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.

The system uses the clients SSO system for authentication and collects the users name and email to display and identify the user in the software over SAML v2.

The system also collects data from training devices such a simulated heart rates to display with the users' training results as these are the devices they are training on over TLS.

The system may also generate scores or other reports to display as part of the users' training results which is done as part of the applications logic.

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

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

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

The information for name and email is provided via the SSO system of the client and trusted as part of the SAML 2 meta data and key exchange.

Data from the simulation training may be reviewed and updated by staff running the trainings.

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

This system is operating under the following legal authorities, which allow us to maintain the information that is involved with this system:
145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS)
VA 76VA05-General Personnel Records (Title 38)
OPM/GOVT–1-General Personnel Records

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: PII for login is sent directly from the clients SSO system. This requires the clients SSO information to be accurate about its users/employees. Accessing of training results by an unauthorized user. If the clients SSO configuration is setup in an incorrect manner, users may be granted incorrect roles within the SimCapture Cloud software.

Mitigation: If the client's data is incorrect the SSO mapping can be reconfigured by the client.

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 SimCapture Cloud system is used for the continuation of education and training of the customer's staff to ensure best practices and best care for the clients patients.

- Name - Analysis of training uptake and training performance by employees of Customer, access to trainings by Customer employees, access to training analysis and reports by Customer employees
- VA Email - Analysis of training uptake and training performance by employees of Customer, access to trainings by Customer employees, access to training analysis and reports by Customer employees
- PIV # - Analysis of training uptake and training performance by employees of Customer, access to trainings by Customer employees, access to training analysis and reports by Customer employees
- Grades - Evidence of training performance and completion, analysis of training performance
- Audio/Video Recordings - Analysis of training performance

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

SimCapture Cloud may produce scoring reports as part of its Enterprise Learning Management feature. This will allow clients to review scores of trainings and identify areas of improvements for induvial leaners. SimCapture Cloud makes various score reports available and highlights scores outside of the standard deviation. It is at the client's discretion to act on these reports or re-implement any trainings. This is not available in the Pro level features of the software as that contains no scoring.

2.3 How is the information in the system secured?

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

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

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

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

All data in and out of the system is transferred over TLS 1.2. There are no SSN or passwords within the system. Internal access to the systems is protected via role-based authentication.

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

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

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

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

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

Laerdal Medical does store student records such as first and last names, emails, and grades. Laerdal Medical does store audio and video records but does not use or create any biometric data from these records. Access to recordings can be limited to only Government Furnished Equipment (GFE) connected to the VA network via Single Sign-On internal (SSOi) limitations. Laerdal Medical's processing of data does include cross-border processing for support and

operations services within the United States. The system supports integration with data-streams from multiple clinical training hardware devices that would be connected to the SimCapture Cloud, provides streamlined training for simulation teams, and mass storage capabilities.

Access to this data is controlled through Laerdal's internal single sign on system, in which authorized users use their named account to access the system. This is done at the clients request and approval for support purposes. All access to data is logged and access is tied directly to the employee. Proper use and access of the systems by Laerdal employees for support and hosting services are the responsibility of the Senior Support Manager, the Senior Cloud Ops Engineer, and their office head the GM and VP of Software development.

Section 3. Retention of Information

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

3.1 What information is retained?

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

All data collected by the system is retained for use in reviewing trainings conducted by the VA. This data includes name, VA email, PIV #, grades, and audio/visual recordings. This data is only removed when and authorized administrator at the VA deletes the data from the system. The system only collects the minimum information needed for the VA to properly review and debrief the trainings and to allow authentication.

3.2 How long is information retained?

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

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

The VA may set their own data rules and policy for data stored within the SimCapture Cloud system in the SimCapture user interface to perform automated deletion of data.

The backup retention policies may be changed for the SimCapture Cloud system if requested by the VA if it does not impact the ability to support and restore the SimCapture Cloud system.

Deleted videos are kept for 24 hours to allow a small window for recovery on accidental deletion by a user. Database and log backups are kept for 90 days.

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.

VHA has proposed the use of the Records Control Schedule 10-1, Item Number:
1100.40 - Educational Activity Records for all electronic data and media files collected and retained by the Laerdal Simulation System.

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

Data will be destroyed in accordance with VA Directive 6500, NIST SP 800-88, and VA Directive 6371.

Electronic data and files of any type, including Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008). When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800- 88r1 as evidenced in the FedRAMP Audit reports.

RQI 1Stop will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the system. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage.

It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws. This system does not use paper records.

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

Yes, the data within the production system is never used for testing. Data used in monitoring of the system for hosting services and research for software improvements does not include PII information.

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.

Follow the format below:
<u>Privacy Risk:</u> Data retention within the system is set by the VA. Data backups are kept for be able to restore the system if the client incorrectly removes data. This is set at 90 days to ensure the client has time to notice this removal and request recovery of the data.

Mitigation: The VA may change the data destruction policies within system to meet any changing requirements. The backups are automatically deleted to ensure they are not kept for longer than necessary, stored in a separate location, and access controlled through IAM roles.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

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

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*

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: No risk is posed as there is no internal sharing of PII.

Mitigation: Mitigation is not needed as there is no privacy risk.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
SimCapture Cloud	To create student profiles, corresponding performance metrics, and grades	First Name, Last Name, VA email, grades, audio/video recordings	MOU/ISA	HTTPS with authentication token

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: PII could be compromised in the transmission to the external SimCapture Cloud.

Mitigation: HTTPS with authentication token is being used to protect the information during transmission.

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.

If the use of video or audio recordings will occur, notice will be provided according to VHA Directive 1078, Privacy of Persons Regarding Photographs, Digital Images, and Video or Audio Recordings https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9547 . Specifically, following guidance on overt production of photographs, digital images or video or audio recordings occurring through a device that is in an area where all persons have awareness and notice that they are subject to photography, imaging or recording. This will be done via posted notice upon entering the learning lab.

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

No, if a user does not wish to provide their information or be in the recordings, they will not be able to login and therefore not use the system.

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

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

No, individuals to not have the right to consent to particular uses of the recordings or information. According to Directive 1078, the Learning Lab would qualify as "Other Areas" and, therefore, there is no need to obtain the written consent of persons in these areas prior to the production of photographs, digital images or video or audio recordings.

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

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

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

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

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: No notice is provided to users of the usen of recording when accessing the Laerdal Simulation System itself.

Mitigation: Mitigation will be provided via posted notice upon entering the learning lab that will be created and mounted consistent with VA signage guidelines found in VHA Directive 1850.05, Interior Design Operations and Management Program, dated September 22, 2017. Additional mitigation is provided by making this Privacy Impact Assessment (PIA) available for review online.

Section 7. Access, Redress, and Correction

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

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

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

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

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

The information in the system is provided through the VA's SSO system and any information from within that system should be addressed with the VA. The VA is the data controller and any information requested by a user that they do not have access to will be redirected to an

administer at the VA to review an act directly on. No PII data is kept or recorded that the VA does not have direct access to or control of.

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

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

The VA has access to correct and update all data within the system. Any requests for such changes by a user that does not have the correct access rights will be directed to an administrator at the VA to act on.

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.

If a user requests an update or change to data they do not have access to they are directed to contact the contracts primary contact at the VA. This is done by the method the user reached out to the SimCapture Cloud team.

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.

If a user requests an update or change to data, they do not have access to they are directed to contact the contract's primary contact at the VA. This is done by the method the user reached out to the SimCapture Cloud team.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: An individual's PII could be incorrect or inappropriately altered within the system.

Mitigation: VA maintains full ownership of data within the system. User requests to update or change data are directed to contact the contract's primary contact at the VA. No PII data is kept or recorded that the VA does not have direct access to or control of.

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 system uses a role-based authentication method to define what information they have access to. How these roles work and how the VA may assign them to users are covered in our user guides.

How users gain access is determined by the VA's SSO system. This may be configured to auto provision users to a certain role type on first login. Alternatively, a VA administrator may manually create or upload a list of users who will have access through the SSO system and what role they have.

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.

SimCapture Cloud is a Software as a Service developed, maintained and supported by Laerdal Medical. Laerdal will only have access to PII if required to provide support at the VA's request from the Support and Cloud Operations Team. All access is done with named and logged accounts with a restrictive role-based system. For example, if there is a request to verify some data, or if a video does not appear to be able to play back. All individuals who operate or access the system sign the National Rules of Behavior; a separate NDA is not required.

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

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

Users are trained on the use of SimCapture Cloud. Users also complete the following VA-specific annual trainings within TMS:

- VA Privacy and Information Security Awareness and Rules of Behavior (WBT) TMS ID 10176
- ISO Led Privacy and Information Security Awareness and Rules of Behavior Presentation TMS ID 832914
- VA Privacy and Information Security Awareness and Rules of Behavior – Print (PDF) TMS OD 31167
- Training Reciprocity: Annual Privacy and Information Training TMS ID 3847875

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

ATO in progress through DTC; categorized at Moderate. The IOC date is 05/31/2023.

Section 9 – Technology Usage

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

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

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

Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

Yes. The system uses cloud technology. There is no current ATO/FedRAMP Authorization for the SimCapture Cloud solution on the application level, however this effort has been initiated. The system has a current data security categorization of Moderate from the VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office. The SimCapture Cloud used in the Laerdal Simulation System-Building 22 Renovation Project 595-15-201 is a Software as a Service.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

The agreement is between the VA and the SaaS solution vendor Laerdal Medical. However, the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is 36C24421P0777.

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.

Yes, the cloud system collects access, usage, and error data which is kept for 90 days. This is used to support, maintain, monitor the health of, and improve the system. This data is owned by Laerdal and used internally for the hosting and support of the system.

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.

The selected CSP inherits the following controls from FedRAMP - Authorized Cloud Infrastructure Provider (Amazon Web Services) that includes:
• Physical and Environmental controls
• Patch Management (on infrastructure level)
• Configuration Management (on infrastructure level)
• Awareness & Training (on infrastructure level)
Service Provider (Amazon Web Services) claims responsibility for protecting the hardware, infrastructure software, networking, and facilities that run AWS Cloud services

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).

The system does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

TONYA HROMCO 372566

Digitally signed by TONYA HROMCO 372566
Date: 2022.02.28 09:23:29 -05'00'

Privacy Officer, Tonya Hromco

Matthew R Schmuck 481358

Digitally signed by Matthew R Schmuck 481358
Date: 2022.02.28 09:38:01 -05'00'

Information Systems Security Officer, Matthew Schmuck

HENNA GROVER

Digitally signed by HENNA GROVER
Date: 2022.03.01 10:30:34 -05'00'

Information Systems Owner, Henna Grover

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).

PRIVACY OF PERSONS REGARDING PHOTOGRAPHS, DIGITAL IMAGES AND VIDEO OR AUDIO RECORDINGS
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9547