Privacy Impact Assessment for the VA IT System called:

Veterans Integrated Implant Application Tracking Solution (VIIATS)

VHA

Date PIA submitted for review:

1/22/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Andrea Wilson	Andrea.Wilson3@va.gov	321-205-4305
Information System Security Officer (ISSO)	Bryan Johnson	Bryan.Johnson@va.gov	801-582-1565 Ext 5443
Information System Owner	Tyke Stewart	Tyke.Stewart@va.gov	909-825-7084

Abstract

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

The Veterans Integrated Implant Application Tracking Solution (VIIATS) is a web-based software application used in the tracking, inventory management and analysis of all implantable devices utilizing Unique Device Identifiers (UDI), as required by FDA and Joint Commission. The system also utilizes Radio Frequency Identification (RFID) and Bar Code Scanning to assist with tracking of implantable devices. This system resides on InVita Healthcare Technologies hosted private servers that are not publicly searchable or accessible and does not utilize cloud technology.
** Note: Champion Medical Technologies d/b/a InVita Healthcare Technologies (henceforth known as InVita)

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?*

VIIATS is a web-based software application used in the tracking, inventory management and analysis of implantable biologic and medical devices. It is intended for use by healthcare providers to meet FDA, Joint Commission and other compliance requirements, improve the accuracy of logging regulatory information for surgical cases, and improve patient safety through the timely notification of recalled or expired implantable. The number of individuals with information to be stored in the system is variable by VA location and can be scaled to accommodate extremely high volumes of data as required.

This system resides on InVita hosted private servers that are not publicly searchable or accessible and does not utilize cloud technology. Data entered or transmitted into the application remains owned by the VA, including PHI and PII where it exists. VIIATS is constructed in such a way to allow minimal storage and transmission of PHI/PHI, specifically requiring only patient medical record number (MRN) and Date of Birth, but VA facilities are able to expand this and store additional PII elements if desired. All data is protected with authentication, encryption and firewall mechanisms regardless of the data type stored or sent to the system, and all information is considered sensitive and/or confidential when handled by InVita representatives or technicians.

The release of privacy related data by accident or malicious intent would have zero, minor or moderate effects, variable based on VA choice to enter additional patient data.
The legal authority to operate this system is: H.R.28 - Biological Implant Tracking and Veteran Safety Act of 2017.

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 (last 4)
☒ 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)

1. First initial last name along with last 4 of Social Security Number.
2. Date of Surgery
3. UDI Device:
a. Lot
b. Serial Number
c. Expiration Date

PII Mapping of Components

VIIATS consists of 6 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by InVita UDI Tracker and the functions that collect it are mapped below.

PII Mapped to Components

Components of the information system (servers)	Does this system collect	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

collecting/storing PII	**PII? (Yes/No)**	**PII? (Yes/No)**			
Products	No	No	N/A	N/A	256-BIT Encryption /Firewalls/Authentication
Inventory	No	No	N/A	N/A	256-BIT Encryption /Firewalls/Authentication
Shipments	No	No	N/A	N/A	256-BIT Encryption /Firewalls/Authentication
Transfers	No	No	N/A	N/A	256-BIT Encryption /Firewalls/Authentication
Suppliers	No	No	N/A	N/A	256-BIT Encryption /Firewalls/Authentication
Cases	Yes		DOB; First initial of last name along with last four of the SSN; Date of Surgery; UDI Device: Lot, Serial Number and Expiration Date	Compliance and Patient Safety	256-BIT Encryption /Firewalls/Authentication

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

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

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

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

The information indicated above is added by VA healthcare provider users or inventory management specialists (receiving dock workers as in the case of receiving shipments), or by the VistA system (future use). There is no need for direct entry by patients since this is not a patient-centric or direct critical care application.
PHI/PII Information in Bold

Inventory(Direct)
1) Product Code
2) Implant Type
3) Family
4) Product Type
5)Product Name
6) ID/Serial Number/Lot
7) Expiration Date
8) Price
9) Quantity

Products(Direct)
1) Implant Type
2) Family
3) Product Type
4) Product Code
5) Suppler
6) Product Description
7) Cost

Shipments(Direct)
1) Date
2) Receive To
3) Purchase Order Number
4) Date Shipped
5) Date Received
6) Time Received
7) Entered by
8) Shipping Integrity
9) Ship Type
10) Ship Temp Maintained
11) Tracking Number
12) Comments

Transfers(Direct)
1) Hospital/Department
2) Storage Department
3) Return to Supplier
4) Product Code
5) ID/Serial Number/Lot
6) RFID Tag Number
7) Date Shipped
8) Comments
9) Received
10) Ship Type
11) Package Integrity
12) Tracking Number/name

Suppliers(Direct)
1) Supplier Type
2) Supplier Name
3) Also known as
4) Supplier Address
5) Supplier City
6) Supplier Zip Code
7) Supplier Phone
8) Supplier Fax
9) Supplier Primary Email
10) Supplier Secondary Email
11) FDA Registration
12) Supplier Model

Cases(Direct)
1) Hospital/Department
2) In OR Time
3) **Surgery Date**
4) **Patient ID**
5) **Birth Date**
6) Procedure
7) Surgeon
8) OR Staff
9) Package Open by
10) Tissue Received by
11) Comments
12) **Product Code**
13) **ID/Serial Number/Lot**
14) RFID Tag Number

VIIATS has its own Analytics system that uses the above data fields for the user to create their own reports. Reports can be created by the individual user of the program with any combination of the data collected.

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.

Information is sent via HL7 communication from VistA surgical package, scanned in from patient wrist band (issued from facility), or typed in manually by the surgical staff.

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 program tracks surgically implantable devices into Veterans. The main purpose of this is to assist with managing recalls of these products. With the PII information being used this process is now done electronically and at a greater speed than ever before. This process previously would take weeks of manual work with a 10 to 20% error rate. Using the VIIATS program, the same research is done in seconds with 100% accuracy. The PII information is used to correctly identify the patients as well as the products.

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.

The information will be checked for accuracy using an audit system comparing the data stored in the system to other records. Before the information can be signed as complete, a second look is performed by the clinical nursing staff and medical provider. The medical staff also performs a "Time Out" procedure to verify the correct information pre-and post-surgery, to check for accuracy.

Accuracy is tracked with limited human input with a greater than a 99.9% electronic information entry and with 100% human-less data entry goal.

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

Unique Device Identification, or UDI, was created to assign a unique identifier to medical devices (e.g. heart valves, hip/knee implants, stents). It was signed into law on September 27, 2007, as part of the Food and Drug Administration Amendments Act of 2007. This Act asked for the creation of a Unique Device Identification System and included the following mandates:

- The label of a device must bear a unique identifier, unless an alternative location is specified by the U.S. Food and Drug Administration (FDA) or unless an exception is made for a device or group of devices (§1271.290(c)).
- The unique identifier must allow identification of the device through distribution and use.
- The unique identifier must include a lot or serial number if specified by FDA

The UDI is composed of a device identifier (manufacturer, catalog, reference number, product description) specific to the device model, and a production identifier (lot or batch number, serial number and/or expiration date) for the specific device. The FDA feels an UDI system can improve the quality of information in the FDA Adverse Event Reporting System (FAERS) thus improving patient safety by finding problem devices more quickly.

Joint Commission standards apply to hospitals that store or issue tissue. This includes any areas outside of the clinical laboratory that store or issue tissue; for example, surgery and outpatient centers or tissue banks. They apply to human and nonhuman cellular-based transplantable and implantable products whether classified by the U.S. Food and Drug Administration (FDA) as a tissue or a medical device.

Collagen and tissue products derived from plastics and polymers are not considered cellular-based products and are not evaluated under these standards.

Specific tissue transplant requirements apply to autologous tissue. This includes policies and procedures for identifying, tracking, storing, and handling autologous tissue, in addition to investigating tissue adverse events. Also, if the state in which an organization resides classifies something as tissue that falls outside the scope of Joint Commission definitions, the standards would apply.

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> When information is stored or collected there is always an element of risk that the information will get compromised.

<u>Mitigation:</u> VIIATS is protected using authentication, encryption, firewalls, monitoring and a wide array of other security tools and measures. Internal and independent testing is conducted on a regular basis to ensure systems remain impenetrable. Risk assessment is conducted on an ongoing basis. The magnitude of harm if data were to be disclosed is low to moderate, depending upon what information the VA chooses to store**.**

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 purpose of collecting the data is to ensure Veterans' implants are recoverable in the case of a recall on such items. This increases patient safety as well as the efficiency of the staff. The use of

RFID tags containing only the tag number and product information are transmitted to the Terso and then to UDI Tracker. This creates a more efficient way to track information.

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

VIIATS's Data Analytics module uses indexed data from cases and inventory inputs to create graphs for easy interpretation by VA Admin users. The data for this information is listed in section 1.2 and can be used by the VA Individual for evaluation the procedures within the department.

2.3 <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.

Add answer here:

Access to PII and PHI is controlled by VA Administrators and can be restricted using the role-based access built into the VIIATS system. Any view or modification of PII/PHI is logged by username, record number, details of the event and date/time. InVita manages general program safeguards and VA Administrators are able to additionally audit the activity related to PII/PHI within the VIIATS program. With regard to VA workers, Access to PII is limited to those who have direct patient care in surgical services along with administrative staff to oversee the program.

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

Inventory(Direct)
1) Product Code
2) Implant Type
3) Family
4) Product Type
5)Product Name
6) ID/Serial Number/Lot
7) Expiration Date
8) Price
9) Quantity

Products(Direct)
1) Implant Type
2) Family
3) Product Type
4) Product Code
5) Suppler
6) Product Description
7) Cost

Shipments(Direct)
1) Date
2) Receive To
3) Purchase Order Number
4) Date Shipped
5) Date Received
6) Time Received
7) Entered by
8) Shipping Integrity
9) Ship Type
10) Ship Temp Maintained
11) Tracking Number
12) Comments

Transfers(Direct)
1) Hospital/Department
2) Storage Department
3) Return to Supplier
4) Product Code
5) ID/Serial Number/Lot
6) RFID Tag Number
7) Date Shipped
8) Comments

Suppliers(Direct)
1) Supplier Type
2) Supplier Name
3) Also known as
4) Supplier Address
5) Supplier City
6) Supplier Zip Code
7) Supplier Phone
8) Supplier Fax

Cases(Direct)
1) Hospital/Department
2) In OR Time
3) Surgery Date
4) Patient ID
5) Birth Date
6) Procedure
7) Surgeon
8) OR Staff

9) Received	9) Supplier Primary Email	9) Package Open by
10) Ship Type	10) Supplier Secondary Email	10) Tissue Received by
11) Package Integrity	11) FDA Registration 1	1) Comments
12) Tracking Number/name	12) Supplier Model	12) Product Code
		13) ID/Serial Number/Lot
		14) RFID Tag Number

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.

Patient Medical Records-VA, SORN 24VA10A7 (Oct. 02, 2020)
If the data is stored in the patient medical record then the retention must be in accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted.

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10 (Dec. 23, 2020, as amended).

All data in the system is kept for an indefinite period of data for recall purposes. Joint Commission requirements indicate that data should be kept for a period of 10 years at minimum. InVita does not purge information on an automated basis, information is kept indefinitely unless upon written request. InVita follow guidelines laid out in, SORN 24VA10A7 (Oct. 02, 2020) which states that electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed or deleted.

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.

Records Control Schedule (RCS) 10-1, November 2017 Paper records and information stored on electronic storage media are maintained and disposed of in accordance with records disposition authority approved
by the Archivist of the United States, and VA policies and procedures for media sanitization, (SORN 24VA10A7 (Oct. 02, 2020)).

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

Any sensitive paper records are shredded on-site to NIST standards. After final disposition, the contractor provides a certificate of destruction. Electronic media containing individually identifiable information is destroyed per NIST guidelines. Defective or damaged magnetic storage media that have been used in a sensitive environment shall not be returned to the vendor (and will be annotated in all contracts/Statements of Work). The IT Area Manager, Information Security Officer (ISO) or designees will be responsible for this process.

Other Data that is not destroyed at the site of production such as that which is transported for destruction, is secured in locked containers or in locked areas until it is removed for destruction. Media in-route to final disposition is rendered unreadable prior to transport. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/. Once the records retention period has been met or records have been otherwise deemed appropriate to destroy, paper records are criss-cut shredded either on-site (for records stored or used at InVita facilities) or sent to a secure shredding provider. Physical media such as hard drives or electronic storage items are electronically wiped/degaussed and then physical destroyed by shattering or bending platters or otherwise demolished. This again may be performed on-site for InVita facility equipment, at the data center, or decommissioned by a secure destruction vendor.

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

VIIATS does not share any information with non-customers with the exception of providing a tool that allows a user to notify a supplier via email that an implant has been used.
Note:
MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES

The organization, where feasible, uses techniques a test site to eliminate the risk of to minimize the risk to privacy of using PII for research, testing, or training. VIIATS has a training program that can be used to train new personal in the use of the product. Any testing of the system is done on the test site and does not use live data. InVita does not send data out to use for research.

VA standard procedures prohibit the use any PII for testing in the development environment and any screen shots shared in end user training material or user guides. The selected development team members and clinicians participating in User Accepting Testing (UAT) are granted elevated privileges for the SQA and Pre-Production environments perform testing and participate in troubleshooting of identified defects.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:
Privacy Risk: There is always a risk that information maintained by VIIATS could be maintained longer than necessary to fulfill the mission.

Mitigation: Data is only retained as necessary for its intended purpose and PII is only retained for as long as necessary and relevant for the purpose for which it was created. Program officials are responsible for disposing of records in their program area in accordance with VA policy SORN 24VA10A7. Staff is required to take the Records Management course via TMS which outlines the process for the retention and purging of data. The VA also follows the Records Control Schedule (RCS) 10-1, November 2017 schedules for each category or data it maintains. When the data retention is reached, data will be disposed of in accordance with the approved method in place at the time.

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***
InVita bilateral communication with	Needed to have data sent between the system in order to fill	1. First initial last name along with last 4	VPN Tunnel / HTTPS Connection

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***
VistA Surgical Package/GIP/PIP	out the required information on the Veterans implants for tracking purposes.	of Social Security Number. 2. Date of Surgery 3. UDI Device: a. Lot b. Serial Number c. Expiration Date	

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

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

Follow the format below:
<u>Privacy Risk:</u> The privacy risk associate with maintaining PII is that sharing data within Department of Veterans Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

<u>Mitigation:</u> The principle of need-to-know is strictly adhered to by the InVita Healthcare Technologies personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: 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***
N/A	N/A	N/A	N/A	N/A

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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: N/A
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.

Notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: Patient Medical Records-VA, SORN 24VA10A7 (Oct. 02, 2020) Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10 (Dec. 23, 2020, as amended).

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.
This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Individuals have the right to decline to provide information; however, the VHA may not be able to enroll the Veteran. The Notice of Privacy Practices states that the Veteran has the right to request a restriction of the use and disclosure of information; however, under 45 CFR § 164.522(a)(1)(vi) the VHA is not required to agree to such a restriction. Employees and VA contractors are also required to provide requested information to maintain employment or contracts with the VASLCHCS.

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

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contests of such record, should submit a written request or copy in person to the last VA health care facility where care was rendered. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI. 24VA 10P2 and 79VA 10P2 states that individuals who wish to contest information in this system of records contains information about them should contact the system or records owner. The Veteran has the right to consent to use of U.S.C. 7332 (Alcohol and Substance Abuse, HIV, and Sickle Cell

Anemia) and medical records by completing the VA Form 10-5345 to authorized third party's information. Treatment, payment, and healthcare operations will require Veteran authorization for the use of U.S.C. 7332 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

Follow the format below:
Privacy Risk: There is a risk that Veterans and other members of the public will not know that information exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them**.**

Mitigation: The VIIATS does not collect information directly from the public. Therefore notice prior to collection would be given at the collection points of the source systems supplying the data. Notice is given through the applicable SORN listed above and this PIA. The risk of the Veteran not receiving "Notice" is low; however, the risk of information being used for another purpose other than what is articulated in the notice is moderate to high, as individuals could mistakenly use information inappropriately. Access controls, physical controls, technical controls, audits/monitors, and ongoing education of information use is active to mitigate risk of information used inappropriately.

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 VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. Each VHA Privacy Act system of records notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. VHA permits individual to obtain access to or get copies of their PII, and this is outlined in VHA policy. Individuals must provide a written request for copies of their records to the VHA facility Privacy Officer for medical records or the System Manager for the Privacy Act system of records as outlines in the notices.

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 are provided the opportunity to submit a request for change in medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer (PO), or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the privacy officer for processing.

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 may request correction of their information by contacting the Facility Privacy Officer, Chief of HIMS and/or the Release of Information Office (ROI). Individuals are provided verbal notice of amendment process by the Privacy Officer.

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.

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

A formal redress process via the amendment process is available to all individuals. In addition to the formal procedures discussed in question 7.3 to request changes to one's health record, a Veteran or other VAMC patient who is enrolled in MyHealthevet can use the system to make direct edits to their health records.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:
Privacy Risk: There is a risk that individual may not know how or who to seek to access or redress records about them held by the VA Office.

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications.

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.

Access to VASLCHCS working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Access is requested per local policies utilizing Network Access Request System (NARS). Users submit access requests based on need to know and job duties. Supervisor and OIT approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need to know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at the VASLCHCS facilities is limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at VASLCHCS or an OIG office location remote from VASLCHCS, is controlled in the same manner.

Only users employed/contracted by the VHA have access to the system. Access digital audit trails are documented through Administrators input when accounts are created, and this access is tracked through the applicable system through logging.

Standard User: Typical employee hired within the facility to perform duties within a specific service. These users can access only the information systems/data required to perform their duties.

OIT Administrator: These users have elevated privileges necessary to perform administrative and system management duties required in OIT operations.

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.

Contractors will have access to the system(s) only for which they have been designated/approved access to per contractual agreements. Contracts are reviewed annually by the Contracting Officer Representative (COR) to determine access requirements. Contractors having access to PHI/PII are required to complete a Business Associate Agreement. Access to the system is dependent upon the contractual requirements for support (i.e. remote server/workstation admin duties). Vendors requesting access to VHA systems are required to undergo background investigations and receive clearance from an ISO prior to account creation. All reviews are conducted by the ISO/CRO.

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

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

All VA staff (employees, volunteers and without compensation (WOCs), residents, students) that need computer access or has access to PII/PHI must complete the annual VA Privacy and Information Security Awareness training and Rules of Behavior and Privacy and HIPAA focused training, in addition there are job specific information trainings that are required for different positions.

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.***

The VIIATS was granted a one year conditional ATO on 19th November 2020. FIPS 199 classification High.

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.

Andrea J. Wilson 104706

Digitally signed by Andrea J. Wilson 104706
Date: 2021.02.23 08:05:15 -05'00'

Privacy Officer, Andrea Wilson

BRYAN L. JOHNSON 1535914

Digitally signed by BRYAN L. JOHNSON 1535914
Date: 2021.02.23 08:07:52 -07'00'

Information Security Systems Officer, Bryan Johnson

Tyke S. Stewart 206116

Digitally signed by Tyke S. Stewart 206116
Date: 2021.02.23 05:57:13 -08'00'

System Owner, Tyke Stewart

APPENDIX A-6.1

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

https://www.oprm.va.gov/docs/Current_SORN_List_01_25_2021.pdf