Privacy Impact Assessment for the VA IT System called:

Stryker SurgiCount Safety-Sponge System Tablet and Software
Northport (NOP) Veterans Affairs Medical Center (VAMC)

Date PIA submitted for review:
October 15, 2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contact</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer (PO)</td>
<td>Dorothy Baker</td>
<td><a href="mailto:Dorothy.Baker3@va.gov">Dorothy.Baker3@va.gov</a></td>
<td>631-261-4400 ext. 4544</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>William Ponce</td>
<td><a href="mailto:William.Ponce@va.gov">William.Ponce@va.gov</a></td>
<td>631-261-4400 ext. 4093</td>
</tr>
<tr>
<td>Information System Owner (ISO)</td>
<td>Fred Tolley</td>
<td><a href="mailto:Fred.Tolley@va.gov">Fred.Tolley@va.gov</a></td>
<td>(202) 461-9005</td>
</tr>
</tbody>
</table>
Abstract

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

Unintended retentions of a foreign object after surgery, especially sponges, remain the most frequently reported events to The Joint Commission (TJC). These serious adverse events have resulted in patient harm involving reoperation, readmission/prolonged hospital stay, infection or sepsis, fistulas/bowel obstructions, visceral perforation, and death. Cotton gauze sponges account for 48–69% of retained surgical items and result in more serious tissue reaction than metal fragments. Because of the complexity of perioperative patient care, the multitude of contributing factors that are difficult to control such as emergency surgery and unplanned changes in procedure, an update to this technology to account for sponges used during surgery is a must.

The SurgiCount Safety-Sponge System Tablet and Software accurately tracks surgical sponges utilizing uniquely identified laparotomy sponges, gauze, and towels to provide real-time count, in conjunction with manual count, so the Operating Room (O.R.) team can confidently close the patient.

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?
The SurgiCount Safety-Sponge System Tablet and Software will consist of 6 SurgiCount tablet kits and SurgiCount 360 software and will be an upgrade to the existing SurgiCount system already in use at the Northport VAMC. This system accurately tracks surgical sponges utilizing uniquely identified laparotomy sponges, gauze and towels to provide real-time count, in conjunction with manual count, so the O.R. team can confidently close the patient. The accompanying software provides accurate post-operative and fully compliant documentation. It allows access to both individual procedure reports and aggregate data to provide auditable evidenced based outcomes and enhanced patient safety.

Features:

1. Tablet:
   a. User-friendly technology
   b. WIFI capability with real-time data transfer to server
   c. Secure cloud-based server/storage
   d. Admin portal for password-protected, VPN access from any onsite or remote computer
   e. Tablet reconciliation with option to capture through software, customizable for post-op compliance/reporting
   f. 10” interactive touch screen
   g. Slip-in battery slot for recharge without shut down or hot swap
   h. Wound-pack reconciliation/closing review
   i. Data Security:
      1. Encrypted data while:
         i. In transit: HTTPS traffic encrypted by signed SSL certificate from trusted certificate authority
         ii. At rest: Data stored in encrypted database
   2. Patient identifiers (random assigned number) are obscured prior to encrypted transmission and storage
   3. Mobile device management system:
      i. Kiosk mode limits user access to sponge counting application only
      ii. Prevents installation of unapproved software on tablet
      iii. Two-step authentication ensures tablet connectivity to correct database
      iv. Password protection ability if tablet is lost or stolen
      v. Data is stored and accessible in SOC 2 certified cloud environment

2. Software:
   a. Provides post-op accounting of each uniquely-identified sponge
   b. Demonstrates compliance to hospital policy or third-party best practices
   c. Supplies evidence-based data for external audits
   d. Generates actionable data for quality initiatives, outcomes percentages, issues resolution or performance optimization
   e. Captures deviations with justifications noted (e.g. wound pack)
   f. Yields objective metrics for inventory, purchasing, budget and staff planning
   g. Enables virtually endless report customization
   h. Data Capture:
      1. Case data downloads into the aggregated SurgiCount360 Software database
      2. Exact time each unique Safety-Sponge was accounted for before and after removal from patient
      3. Type of procedure, procedure length and procedure sponge usage
4. Staff changes during procedure (e.g. who exited, who entered and times)
5. Sponge discrepancies and reason (e.g. wound pack, case cancellation)
6. Surgical staff
7. Time of day
8. Patient ID (random assigned number)

3. Sponges and Towels:
   a. Each sponge or towel has its own individual barcode for 100% identification accuracy
   b. Each pack has a unique master tag barcode containing data for all sponges within; also enables a quick “IN” count
   c. Triggers an audible and visual recognition cue for each item scanned
   d. SAFE-T Lap’s barium strip plus radiopaque threads enhance x-ray detectability over barium strip alone
   e. Uses universally-trusted barcode technology which also supports compliance with the FDA’s UDI mandate
   f. Polyurethane Teflon tag wicks away blood and fluids for easy scanning, and can be successfully scanned even with fluid present

The SurgiCount Safety-Sponge System Tablet and Software will scan the patient ID bracelet to obtain the name, ss# DOB of patient, then a random number will be assigned for individual procedure reports and aggregate data. The information scanned from the patient ID bracelet (patient name, SS#, DOB) is not stored in the system. The random number assigned will be obscured prior to encrypted transmission and storage.

Vendor does not have access to the VA server.

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://www.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 (SSN)
- Date of Birth (DOB)
- Mother’s Maiden Name

Version Date: May 1, 2021
Data Capture elements:

1. Case data downloads into the aggregated SurgiCount360 Software database
2. Exact time each unique Safety-Sponge was accounted for before and after removal from patient
3. Type of procedure, procedure length and procedure sponge usage
4. Staff changes during procedure (e.g. who exited, who entered and times)
5. Sponge discrepancies and reason (e.g. wound pack, case cancellation)
6. Surgical staff names
7. Time of day
8. Patient ID (random assigned number)
9. Employee email addresses

PII Mapping of Components

The SurgiCount Safety-Sponge System Tablet and Software consists of one database (tablet & cloud). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Stryker SurgiCount Safety-Sponge System and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>SurgiCount Safety-Sponge System Tablet and Software</td>
<td>Yes</td>
<td>Yes</td>
<td>Employee Names – random</td>
<td>Patient identification</td>
<td>Password protected</td>
</tr>
</tbody>
</table>
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.

This information is collected verbally directly from the patient and directly from their ID bracelet. From staff present at the time of procedure.

Unintended retentions of a foreign object after surgery, especially sponges, remain the most frequently reported events to The Joint Commission (TJC). These serious adverse events have resulted in patient harm involving reoperation, readmission/prolonged hospital stay, infection or sepsis, fistulas/bowel obstructions, visceral perforation, and death. Cotton gauze sponges account for 48–69% of retained surgical items and result in more serious tissue reaction than metal fragments. Because of the complexity of perioperative patient care, the multitude of contributing factors that are difficult to control such as emergency surgery and unplanned changes in procedure, an update to this technology to account for sponges used during surgery is a must.

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?
Information from individuals is collected verbally from the patient. The SurgiCount Safety-Sponge System Tablet and Software will scan the patient ID bracelet to obtain the name, SS# and DOB of patient, then a random number will be assigned for individual procedure reports and aggregate data. The information scanned from the patient ID bracelet (patient name, SS#, DOB) is not stored in the system. The random number assigned to the patient will be obscured prior to encrypted transmission and storage.

Staff enter names, time in/out of procedure, the employee ID is scanned as they open/used/discard items during the procedure.

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.

Information from individuals is collected verbally from the patient. Staff verbally check two patient identifiers for all clinical procedures. Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary.

Errors/discrepancies in any reports are emailed directly to the OR Nurse Manager for mitigation or follow-up. The random number assigned is identified as the case number.

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.
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Veterans’ Benefits, Title 38, United States Code, Sections 501(b) and 304, Title 5, United States Code, section 301
Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

Patient Medical Records-VA, SOR 24VA10A7, The paper and automated records may be used for such purposes as: ongoing treatment of individuals and patients; documentation of treatment provided; payment; health care operations such as producing various management and patient follow-up reports; responding to patient and other inquiries; for epidemiological research and other health care related studies; statistical analysis, resource allocation and planning; providing clinical and administrative support to patient medical care; determining entitlement and eligibility for VA benefits; processing and adjudicating benefit claims by Veterans Benefits Administration Regional Office (VARO) staff; for audits, reviews, and investigations conducted by staff of the health care facility, the networks, VA Central Office, and the VA Office of Inspector General (OIG); sharing of health information between and among Veterans Health Administration (VHA), Department of Defense (DoD), Indian Health Services (IHS), and other government and private industry health care organizations; quality assurance audits, reviews, and investigations; personnel management and evaluation; employee ratings and performance evaluations; and employee disciplinary or other adverse action, including discharge; advising health care professional licensing or monitoring bodies or similar entities of activities of VA and former VA health care personnel; accreditation of a facility by an entity such as the Joint Commission (TJC); and notifying medical schools of medical students’ performance and billing.

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


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: The SurgiCount Safety-Sponge System Tablet and Software contains protected health information on Veterans. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: VHA and NVAMC already deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. Region 4’s security measures include: access control; configuration management; media protection; system and service acquisition; audit and accountability measures; contingency planning; personnel security; system and communication protection; awareness and training; identification authentication; physical and environmental protection; system information integrity; security assessment and authorization; incident response; risk assessment; planning and maintenance.

NVAMC employs all security controls in the respective high impact security control baseline unless a specific risk based decision has been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37, VA handbook 6500, and other specific VA directives.

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.
Much of the information collected is maintained, used, and disseminated to ensure that Veterans obtain the medical health treatment they require. This system will ensure that all items used in the O.R. is tracked and accounted for, minimize adverse events. The report can be linked back to the correct patient.

Errors/discrepancies in any reports are emailed directly to the OR Nurse Manager for mitigation or follow-up on the case. The random number assigned is identified as the case number.

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.

Aggregate data is not obtained or used. Individual data is reviewed for abatement of possible errors and closure of case. These reports/records are not placed in the patient medical file.

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?

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

Admin portal for password-protected, VPN access from any onsite or remote computer.

Data Security:
- Encrypted data while:
  - In transit: HTTPS traffic encrypted by signed SSL certificate from trusted certificate authority
  - At rest: Data stored in encrypted database

The SurgiCount Safety-Sponge System Tablet and Software will scan the patient ID bracelet to obtain the name, SS#, DOB of patient, then a random number will be assigned for individual
procedure reports and aggregate data. Patient identifiers (random assigned number) are obscured prior to encrypted transmission and storage.

Microsoft (Azure) is the cloud service provider. There is an enterprise agreement in place with them. Contained within the patient from our SAAS service and increment the sponge count accordingly. This will help ensure all sponges including the wound packs are identified/removed during this procedure.

### 2.4 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Northport employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments; configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. Northport employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

All employees with access to Veteran’s health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.
The System of Records Notice (SORN) Patient Medical Records-VA, SOR 24VA10A7, is a consolidated health record (CHR) that may be used for such purposes as: Ongoing treatment of the patient; documentation of treatment provided; payment; health care operations such as producing various management and patient follow-up reports; responding to patient and other inquiries; for epidemiological research and other health care related studies; statistical analysis, resource allocation and planning; providing clinical and administrative support to patient medical care; determining entitlement and eligibility for VA benefits; processing and adjudicating benefit claims by Veterans Benefits Administration Regional Office staff; for audits, reviews, and investigations conducted by staff of the health care facility, the networks, VA Central Office, and the VA Office of Inspector General (OIG); sharing of health information between and among VHA, DoD, Indian Health Services, and other government and private industry health care organizations; law enforcement investigations; quality assurance audits, reviews, and investigations; personnel management and evaluation; employee ratings and performance evaluations; and employee disciplinary or other adverse action, including discharge; advising health care professional licensing or monitoring bodies or similar entities of activities of VA and former VA health care personnel; accreditation of a facility by an entity such as the Joint Commission (JC); and notifying medical schools of medical students performance and billing.

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*

- Employee Email Address: used for communication for reports generated
- Surgical staff names
- Patient ID (random assigned number)/ Case # for follow-up of any errors or closure of reports

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.*
When managing and maintaining VA data and records, NVAMC will follow the guidelines established in VA Record Control Schedule (RCS)-10 and in General Records Schedule (GRS). The link to the RCS-10-1 schedule can be found at the following website: Records Control Schedule 10-1 (va.gov)

and the link for the GRS is: http://www.archives.gov/records-mgmt/grs.html

Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care, Department of Veterans Affairs Record Control Schedule (RCS)-10.

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.

When managing and maintaining VA data and records, Northport VA Health Care System will follow the guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS)10-1 and in the General Records Schedules (GRS).

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014), Directive_6371_8_Apr_2014.pdf

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/viewPublication.asp?Pub_ID=416&FType=2

When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is shredded or sent out for destruction per VA Handbook 6500.1. Digital media is destroyed by autoclave or sent out for destruction per VA Handbook 6500.1.
3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. 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.

Vendor will provide initial training to staff on use of the system. The SurgiCount Safety-Sponge System Tablet and Software System is not utilized in research. The data may be used for approved research purposes.

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:** The information scanned from the patient ID bracelet will then be assigned a random number for retained is needed to correctly identify the patient and processes during procedures. There is minimal risk as the information will be instantly assigned a random number.

**Mitigation:** All employees with access to Veteran’s health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the
technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.

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 3.10 (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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:** Not applicable

**Mitigation:** Not applicable

### Section 5. External Sharing/Receiving and Disclosure

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

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

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

**NOTE:** Question 3.11 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
</table>

Version Date: May 1, 2021

Page 16 of 35
<table>
<thead>
<tr>
<th>program office or IT system</th>
<th>sharing (can be more than one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SurgiCount Safety-Sponge System Tablet and Software</td>
<td>System accurately tracks surgical sponges utilizing uniquely identified laparotomy sponges, gauze &amp; towels to provide real-time count, in conjunction with manual count, so the O.R. team can confidently close the patient. Patient report (random assigned number for ID) - case #, employee email address, Exact time each unique Safety-Sponge was accounted for before and after removal from patient, Type of procedure, procedure length and procedure sponge usage, Staff changes during procedure (e.g. who exited, who entered and times), Sponge discrepancies and reason (e.g. wound pack, case cancellation), Surgical staff, Time of day</td>
</tr>
</tbody>
</table>

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

See Section 8.1 and 8.3 that list the specific measures that meet these requirements.

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.

Version Date: May 1, 2021
Page 17 of 35
Follow the format below:

**Privacy Risk:** The sharing of data is necessary for the medical care of individuals account for sponges/items used during surgery is a must. If the information is shared outside of the department there is very minimal risk as the data is coded.

**Mitigation:** The SurgiCount Safety-Sponge System Tablet and Software admin portal is password-protected, VPN access from any onsite or remote computer. Data Security: Encrypted data is in transit and at rest: Data stored in encrypted database

### 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.*

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. The NOPP may be accessed here - [https://research.cuanschutz.edu/docs/librariesprovider148/comirb_documents/va-forms/vha-nopp-7-19.pdf?sfvrsn=5ca13bb9_0](https://research.cuanschutz.edu/docs/librariesprovider148/comirb_documents/va-forms/vha-nopp-7-19.pdf?sfvrsn=5ca13bb9_0)

Patient Medical Records-VA, SOR 24VA10A7 may be accessed - [https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf](https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf)

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

Northport VAMC only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The patient will have an opportunity and has a right to decline to provide the information that the SurgiCount Safety-Sponge System Tablet and Software tracks. This may prevent them from utilizing this important safety feature of their procedure.

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

Yes. Individuals must submit in writing to their facility PO. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out.

Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain 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 the Northport VAMC exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.
Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the “office concerned,” the request may be addressed to the PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as “Privacy Act Request” and notify the requester of the referral.

When requesting access to one’s own records, patients are asked to complete VA Form 10-5345a: Individuals’ Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at https://www.va.gov/find-forms/about-form-10-5345a/.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealtheVet program, VA’s online personal health record. More information about MyHealtheVet is available at https://www.myhealth.va.gov/index.html.
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 required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A.

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.*

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

**Right to Request Amendment of Health Information.**

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.
Additional notice is provided through the SORS listed in 6.1 of this PIA and through the area Release of Information Office where care is received.

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 ensure data accuracy.

In addition to the formal procedures discussed in question 7.2 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 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: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: Northport VAMC mitigates the risk of incorrect information in an individual’s records by authenticating information when possible using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient’s medical appointments.
As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one’s records.

The Northport VAMC Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans’ Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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.

Individuals receive access to the Northport VAMC by gainful employment in the VA or upon being awarded a contract that requires access to the Area systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. Northport VAMC requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

Access is requested utilizing Electronic Permission Access Area Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T 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 Northport VAMC is generally limited by appropriate locking devices and restricted to authorized VA IT employees. 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 the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.

Access to the Northport VAMC 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 System Security Officer (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Human Resources notify Divisions, IT and ISSO of new hires and their start date(s) through email. The Division that the person is going into fills out the local access form, Automated Systems Access Request form, with name, SSN and/or claim number, job title, division and telephone number, along with marking the boxes on the form for application access the user will need on the computer system. This form starts at the Division level, is signed by the Division Chief, then goes to the ISSO and Director, for signatures and then to IT for implementation. Documentation is filed in an employee folder and maintained in the ISSO’s office.

- Individuals are subject to a background investigation before given access to Veteran’s information.
- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually AND Privacy and HIPAA Focused Training.

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.

The Vendor does not have access to the VA server.
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 Northport VAMC personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rules of Behavior (RoB) training, during New Employee Orientation (NEO) or via Talent Management System (TMS). In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the area Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information System Security Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained.

The TMS offers the following applicable privacy courses:

- VA 10176: Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPPA Training
- VA 20152: VHA Mandatory Training for Transitory, Part-time and Intermittent Clinical Staff
- VA 3192008: VHA Mandatory Training for Trainees – Refresher
- VA 3185966: VHA Mandatory Training for Trainees -Initial
- VA 3812493: Annual Government Ethics

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.
No, the SurgiCount Safety-Sponge System Tablet and Software needs to undergo review – estimated IOC date of 1 April 2022. The SurgiCount Safety-Sponge System Tablet and Software currently undergoing the FedRamp approval process.

**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, 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.*

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

Microsoft (Azure) is the cloud service provider. There is an enterprise agreement in place with them. The SurgiCount Safety-Sponge System Tablet and Software is currently undergoing the FedRAMP process. The Data Security Categorization is designated as moderate.

### 9.2 Identify the cloud model being utilized.

*Example: 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.*

Software as a Service (SaaS)

### 9.3 Does the contract with the Cloud Service Provider (CSP), 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.*

VA retains ownership of all VA data.

Contract # 36C24220D0071- P00001–amended to include Appendix C of VA 6500.6 Handbook, VA Information and Information Security/ Privacy language, pending signature of vendor, Stryker.

**Section 3. VA INFORMATION CUSTODIAL LANGUAGE**

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in
performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered CREATED by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated, and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above-mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

9.4 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.*

VA maintains ownership of the ancillary data.

There is medi-data collected from the system, date and time stamp. This information is utilized for any troubleshooting of the system.

9.5 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.*

*See Section 5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE of the amended contract.*
a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, Certification and Accreditation and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.
e. The contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA’s network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

(1) Vendor must accept the system without the drive;

(2) VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

(3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

(4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data
folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

9.6 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 SurgiCount Safety-Sponge System Tablet and Software does not utilize RPA.
### Section 9. References

#### Summary of Privacy Controls by Family

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

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

Dorothy Baker
297905
Digitally signed by Dorothy Baker
Date: 2021.10.25 17:03:04 -04'00'

Privacy Officer, Dorothy Baker

William Ponce
1698723
Digitally signed by William Ponce
Date: 2021.10.26 07:00:49 -04'00'

Information Systems Security Officer, William Ponce

FRED TOLLEY
Digitally signed by FRED TOLLEY
Date: 2021.10.26 08:41:17 -04'00'

System Owner, Fred Tolley
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://research.cuanschutz.edu/docs/librariesprovider148/comirb_documents/va-forms/vha-nopp-7-19.pdf?sfvrsn=5ca13bb9_0