Privacy Impact Assessment for the VA IT System called:

National Surgery Office IT System

Veterans Health Administration

Date PIA submitted for review:

09/06/2023

VA System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Sharon Gainey	Sharon.gainey2@va.gov	918-577-3920
Information System Owner	Mark A. Wilson, MD, PhD, National Director of Surgery	Mark.Wilson5@va.gov	202-709-0951

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 Health Administration (VHA) National Surgery Office (NSO) IT System supports the NSO in performing its charge of promoting and ensuring the delivery of high quality, efficient, and Veteran-centric care and surgical services, as well as providing operational oversight of clinical and quality improvement activities. While there are many components to the NSO IT System to accomplish this goal, the Privacy Impact Assessment herein will focus on the 4 components that collect or use Sensitive Health Information (SHI). There are 3 Minor applications: (1) The VA Surgical Quality Improvement Program (VASQIP) system component includes the collection, storage, analysis, and reporting of VA surgical data. Surgical data is utilized to monitor and report risk-adjusted surgical outcomes and unadjusted mortality for surgical procedures performed at VA medical centers with the objective of evaluating the quality of VHA surgical programs and for ongoing improvements to promote Veteran health care. (2) To assure the quality of data collected, the NSO utilizes an Inter-Rater Reliability (IRR) program that compares case assessments for accuracy and consistency. For the IRR, a select number of patient cases are extracted from the VASQIP dataset by the NSO, and the case assessments are provided to a VISN Lead Surgical Nurse who assesses the cases and reconciles differences with the original SQN. (3) The NSO IT System also includes patients who receive Mechanical Circulatory Assist Device (MCAD) surgical implantation. This dataset includes the date of surgery, type of device implanted, and surgical outcomes, which may be referenced for reimbursement amounts to the appropriate facility. There is 1 Major application: (4) The system includes the VHA National Transplant Program patient referral and cost reimbursement information. This component is called Transplant Referral and Cost Evaluation/ Reimbursement (TRACER), which securely manages transplant candidate referrals, evaluation, and surgery information among VA referring hospitals, VA Transplant Centers, and the NSO.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

National Surgery Office (NSO) IT System, Enterprise Management Program Office (EMPO)

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

The primary purpose of the National Surgery Office IT System is to support the NSO in performing its mission of promoting and ensuring the delivery of high quality, efficient, and Veteran-centric surgical care and services, as well as providing operational oversight of clinical and quality improvement activities. This is accomplished through collection, data quality evaluation, storage, analysis, and reporting of VA surgical data as part of the VA Surgical Quality Improvement Program (VASQIP). Surgical data is utilized to monitor and report risk-adjusted surgical outcomes and unadjusted mortality for surgical procedures performed at VA medical centers for all operations combined, and for each surgical specialty, on a quarterly and rolling 12-month basis, with the

objective of evaluating the quality of VHA surgical programs and for ongoing improvements to promote Veteran health care. To assure the quality of data collected, the NSO utilizes an Inter-Rater Reliability (IRR) assessment for clinical care provider verification of accuracy. The National Surgery Office IT System also contains a module which includes patients who receive Mechanical Circulatory Assist Device (MCAD) surgical implantation, as well as a component for Transplant patient referral and cost reimbursement (TRACER) which securely manages the data flow for transplant candidate evaluation, referrals, and surgery information among VA referring hospitals, VA Transplant Centers, and the NSO.

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

VA Owned and VA Operated IS

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

Currently, the National Surgery Office IT System stores information for approximately 9 million Veterans, with approximately 400,000 new patient records added each year. The system includes Sensitive Health Information (SHI) which is Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).

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

The National Surgery Office IT System contains patient-level data from those VA facilities with approved surgery programs as well as VA referring hospitals for transplant surgery patients. The system's data includes Veteran patient demographics; referral, admission, and discharge information; and preoperative, intraoperative, and postoperative clinical data; as well as financial reimbursement information for transplant services. VA key personnel lists include names, titles, and work contact information of those involved with NSO and approved surgical programs. PHI, PII, and III data is pulled by/pushed to NSO for the NSO IT System through various secure intra-VA transmissions depending upon the data source, including:(1)from the VistA Surgical Package, as well as VistA clinical, diagnostic, laboratory, CPT, and demographic data sources through encrypted zip files attached to emails and VA Mailman messages; (2) from Corporate Data Warehouse (CDW) for preoperative, intra-operative, postoperative, hospitalization, discharge, mortality, and readmission records through Microsoft SQL Server Management Studio (MS SSMS), a SSIS job, and SAS.

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

PHI, PII, and III data is pulled by/pushed to NSO for the NSO IT System through various secure intra-VA transmissions depending upon the data source, including:(1)from the VistA Surgical Package, as well as VistA clinical, diagnostic, laboratory, CPT, and demographic data sources through encrypted zip files attached to emails and VA Mailman messages; (2) from Corporate Data Warehouse (CDW) for preoperative, intra-operative, postoperative, hospitalization, discharge, mortality, and readmission records through Microsoft SQL Server Management Studio (MS SSMS), a SSIS job, and SAS.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The system owner is the VHA National Surgery Office. The major and minor applications of the NSO IT System reside on a series of virtual servers that are hosted and maintained by VA OI&T in St. Louis, Missouri. The VASQIP database resides on a SAS server hosted by VA OI&T in Austin, TX. The applications comprise a centralized and unified data collection, analysis, and reporting system maintained solely at the NSO Program Office.

3. Legal Authority and SORN

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

Health information is required pursuant to the general purpose of the program and in order to comply with Public Law 99-166. SSN is required for verification of patient death status, as authorized under the Veterans Administration Health Care Amendments of 1985 (Public Law 99-166), which mandates the VHA to report surgical outcomes data annually. Additionally, Executive Order 9397 as well as Title 38 USC 501 gives authority to collect the SSN.

The system is covered by SORN121VA10 National Patient Databases-VA. 2023-07638.pdf (govinfo.gov) AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C 501.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No, the system is not in the process of being modified and does not require amendment or revision.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No business processes are anticipated with the completion of this PIA.

K. Whether the completion of this PIA could potentially result in technology changes

No technology changes are anticipated with the completion of this PIA.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

The NSO IT System contains patient-level data for Veterans having surgery at an approved VHA surgical program as well as those patients being considered for transplant surgery. The system's data includes Veteran patient demographics: referral, admission, and discharge information: preoperative, intraoperative, and postoperative clinical data, dates of surgical events, and date of death; adverse events; as well as financial reimbursement information for transplant services. VA key personnel lists include names, titles, and work contact information of those involved with NSO and approved surgical programs.

Administrative data in the NSO IT System includes clinic, operating room and ICU facility counts, resident counts, acute care and ICU facility mortality ratios, surgical case reports, and national utilization management results, clinic access and appointments, staff cost and productivity information, inpatient satisfaction results, and staff satisfaction results. Of this data, the SPI within the System are patient names, date of birth, addresses, phone numbers, SSNs, and dates related to surgical events, which are received from VistA and CDW, as well as entered by healthcare coordinators into NSO applications MCAD Tracker and TRACER. Collection, use, and maintenance of SPI by the National Surgery Office IT System is protected by HIPAA.

PII Mapping of Components (Servers/Database)

The NSO IT System consists of 4 key components (servers/databases): VASQIP, IRR, MCAD, and TRACER. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the NSO IT System and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VASQIP (data stores = CICSP, NSQIP, and NSO_DW)	**Yes**	**Yes**	Patient name, SSN, address, phone #, date of birth, date of death, and dates of surgery events	To match surgical case records against internal and external (e.g. Master Veteran Index) data sources at the patient level	Restriction of access to PII to NSO staff with required security training & need PII to fulfill responsibilities
IRR	**Yes**	**Yes**	Patient SSN, Date of Surgery	To match surgical case records against internal VistA data sources at the patient level	Restriction of access to PII to NSO staff with required security training & need PII to fulfill responsibilities
MCAD Tracker	**Yes**	**Yes**	Patient Name, SSN, Date of Birth, Date of Surgery	To match surgical case records against internal VistA data sources at the patient level	Restriction of access to PII to NSO staff with required security training &

					need PII to fulfill responsibilities
TRACER	**Yes**	**Yes**	Patient name, SSN, date of birth, date of death, and dates of referral & surgery events	To match transplant records against internal and external (e.g. Master Veteran Index) data sources at the patient level	Restriction of access to PII to NSO staff with required security training & need PII to fulfill responsibilities
NSOSystems	**Yes**	**Yes**	First name, Last name, Domain Login ID, Email address, Telephone number	To perform Key Personnel role verification and VAMC location identification for providing sensitive surgical information to approved VHA personnel and NSO staff	Restriction of access to PII to NSO staff with required security training & need PII to fulfill responsibilities

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

For components with SPI:

For the VASQIP related NSO IT System components, CICSP (Continuous Improvement in Cardiac Surgery Program), NSQIP (National Surgical Quality Improvement Program), and NSO_DW (NSO Data Warehouse), data is electronically pulled or pushed from VistA and CDW. These sources are utilized instead of direct provider input, since some of the data required by the NSO is already available in the VA medical record.

Other VASQIP data is retrieved from the Surgical Risk Assessment (SRA) database that is a compilation of VistA Surgery records from all VA surgical programs.

For the IRR (Inter-Rater Reliability program) component, data is collected from VistA and from direct entry by VHA surgical quality nurses and VISN lead surgical nurses as IRR Program participants. This information pertains to Veterans.

For the TRACER (Transplant Referral and Cost Evaluation/Reimbursement) component, data is collected through direct entry by transplant coordinators and program administrators at VA referring and transplant centers. This information pertains to Veterans.

For the MCAD Tracker (Mechanical Circulatory Assistance Device Implant Activity/Reimbursement Tracking) component, data is collected through direct entry by health care coordinators at participating VA surgical facilities. This information pertains to Veterans.

For components without SPI:

Other administrative data with summary information about surgical programs is received from various VHA Program Offices including Office of Academic Affiliations (OAA), Inpatient Evaluation Center (IPEC), VHA Support Service Center (VSSC), Managerial Cost Accounting Office (MCAO), VHA Office of Quality & Patient Safety, and National Center for Organization Development (NCOD). VHA Surgical Program facilities also directly report on administrative data including Clinic, Operating Room, and ICU counts and resources, Surgical Infrastructure Inventory facility resources, the number of new patients seen within 30 days clinic metric, documentation for Organ Procurement and Donation After Circulatory Death policy compliance, and alert notifications for critical incidents occurring in the surgical setting. This information pertains to Veterans.

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

Information created with no PHI/PII:
1. NSO Quarterly Report
2. NSO Annual Surgery Report
3. NSO Operating Room Reports (Power BI)
4. NSO Transplant Quarterly Report
5. TRACER Transplant Activity Summary reports
6. Critical Incident Tracking Notification (CITN)
7. Clinic & Operating Room & ICU Resources counts
8. Enhancing Surgical Access Tool (ESAT) report
9. Mechanical Circulatory Assist Device (MCAD) report
10. Operative Complexity & CPT Lookup
11. Organ Procurement Organization | Donation after Circulatory Death (OPO-DCD) verification report
12. NSO Risk Calculator
13. Invasive Procedure Infrastructure Inventory Tool (IPIIT) report
14. VHA Inpatient Evaluation Center (IPEC) output: Division-level O/E ratios
15. VHA Support Service Center (VSSC) output for Network Director Performance Plan: adverse event report
16. Clinical Inventory output: Surgical procedure case counts by division and specialty category and Specialty surgical programs by division
17. Office of Academic Affiliation (OAA) output: surgical procedure case counts by complexity, specialty, division, and level of resident supervision
18. Ad hoc analyses (e.g., FOIA, OSC, OMI, OIG, SVAC, HVAC)

Information created with PHI/PII:
1. NSO Data Viewer reports
2. VA Surgical Quality Improvement Program Case Assessment Status reports
3. TRACER Transplant Patient Activity reports
4. Mechanical Circulatory Assist Device (MCAD) patient implant report
5. Interrater Reliability (IRR) case assessment list
6. Ad hoc analyses (e.g., FOIA, OMI, OIG, SVAC, HVAC, VHA EIC)
7. Research datasets for VA National Data System's VINCI research repository

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

For components with SPI:

Data is collected on surgical cases from the VistA Surgical Package by electronic data extracts through) encrypted zip file email attachments from the SRA database and VA Mailman messages on a scheduled basis five times each quarter for the VASQIP components and the IRR component (when applicable).

Data is collected on patient mortality status from the CDW Master Veteran Index database table. In addition, Vital Status data is electronically pulled from the CDW MS SQL Server database.

Data is collected on patient preoperative, intra-operative, postoperative, hospitalization, discharge, and readmission from the CDW by electronic pull through SSMS and SAS on a quarterly basis. In addition, a subset of patient preoperative, intra-operative, postoperative, hospitalization, and discharge data is pulled daily from the CDW utilizing an SSIS job.

Data is collected on IRR surgical assessments by VA surgical quality nurses and VISN lead surgical nurses via direct system entry into an SSL (Secure Sockets Layer) protected, access-restricted user interface to the IRR Program.

Data is collected for transplant surgery patients by VA clinical care providers at VA referring facilities and transplant centers via direct system entry into an SSL (Secure Sockets Layer) protected, access-restricted user interface termed TRACER.

Data is collected for mechanical circulatory assist device (MCAD) implant surgery by VA clinical care providers at VA surgical program via direct system entry into an SSL (Secure Sockets Layer) protected, access-restricted user interface termed MCAD Tracker.

For components without SPI:

OAA: Excel workbook distributed via e-mail.

IPEC: SAS dataset distributed via shared folder on secure server.

VSSC: SQL Server Reporting Services (SSRS) report is pulled from the VSSC website (https://vssc.med.va.gov/surgery/surgery.aspx); the National Utilization Management Integration (NUMI) results report from Patient Utilization cubes (https://vssc.med.va.gov/VSSCMainApp/); and clinic access and appointment results report from Patient Access and Eligibility cubes (https://vssc.med.va.gov/VSSCMainApp/).

MCAO: SSRS report pulled from the MCAO website (https://mcareports.va.gov/vhaansur.aspx).

VHA Office of Quality & Patient Safety: Excel workbooks downloaded from the SHEP website http://vaww.car.rtp.med.va.gov/programs/shep/shepReporting.aspx.

NCOD: SAS dataset distributed via e-mail.

VHA Surgical Program Facilities: Direct entry into SSL VA intranet portals: CITN, Clinic-OR Resources, ESAT, OPO-DCD verification, IPPIT, VASCAR.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

For the VASQIP component, the NSO IT System relies primarily on internal checks for data accuracy employed by these systems. Additionally, the NSO employs a "VA Surgical Quality Improvement Program Case Assessment Status report" application to provide feedback on data completeness and accuracy issues. This application analyzes surgical case assessment data received from VA surgical facilities in terms of data completeness and consistency. These data accuracy Status reports are performed monthly, with an additional data accuracy report performed quarterly. Any detected gaps or potential inconsistencies are reported to the surgical facility personnel specifically responsible for entering surgical data into the VistA system. VistA surgical case record updates in response to reported data problems are retransmitted to the NSO. If these retransmissions are received prior to the data transmission deadline for the fiscal year in which the surgery occurred, they will automatically update their associated NSO IT System records accordingly. Furthermore, the NSO utilizes an Inter-Rater Reliability (IRR) program to assure the quality of data collected, whereby the nurse reviewers independently provide case data reviews for matching and verifications. An IRR is performed for an individual surgical program on an ad hoc basis when a data accuracy concern is raised.

For the TRACER component, the NSO IT System relies on transplant coordinators and transplant program administrators to provide accurate and internally consistent input, with data quality checks built into the system to alert for missing variables and out-of-range values. The data accuracy reviews may be performed ongoing as the data entry immediately flags for potential erroneous values. Moreover, volume and activity feedback reports are provided within the system for Transplant coordinators and administrators to perform internal validation; these are performed monthly. Synchronization with Vital Status/Master Veteran Index mortality database is performed quarterly to assure data accuracy.

For the MCAD Tracker component, the NSO IT System relies on MCAD healthcare coordinators to provide accurate and internally consistent input, with data quality checks built into the system to alert for missing variables and out-of-range values. The data accuracy reviews may be performed ongoing as the data entry immediately flags for potential erroneous values. Moreover, volume and activity feedback reports are provided within the system for MCAD healthcare coordinators to perform internal validation; these are performed monthly. Synchronization with Vital Status/Master Veteran Index mortality database is performed quarterly to assure data accuracy.

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

Health information is required pursuant to the mission of the NSO and in order to comply with Veterans Administration Health Care Amendments of 1985 Public Law 99-166, 38 USC 4151 "Quality assurance program," which establishes and conducts a comprehensive program to monitor and evaluate the quality of healthcare furnished by the Department of Medicine and Surgery: "… (to) evaluate whether there are significant deviations in mortality and morbidity rates for surgical procedures performed by the Department of Medicine and Surgery from prevailing national mortality and morbidity standards for similar procedures; and … to collect data and other information on mortality and morbidity … for each type of surgical procedure performed by the Department and (with respect to each such procedure) compile the data and other information so collected… and analyze any deviation between such rates and such standards in terms of the (i) the characteristics of the respective patient populations; (ii) the level of risk for the procedure involved….and (prepare) Quality-assurance reports;" as well as management of the VA Transplant Program under VHA Directive 2012-018(1) "Solid Organ and Bone Marrow Transplantation" and VHA Directive 1102.08 "Heart Failure Treatment Utilizing a Ventricular Assist Device or Total Artificial Heart: Patient Selection and Funding".

There is one System of Record Notices (SORNs):

SORN 121VA10 - 'National Patient Databases-VA", which is published in the Federal Register and online: 2023-07638.pdf (govinfo.gov)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
The system's surgical data includes Veteran patient demographics; referral, admission, and discharge information; and preoperative, intraoperative, and postoperative clinical data; as well as financial reimbursement information for mechanical circulatory device and transplant services. Only data that is required for performing the primary tasks of the NSO in accordance with its mission (surgical risk analysis, surgical risk model development/maintenance, risk-adjusted surgical outcomes/unadjusted mortality reporting, transplant referral & reimbursement administration, device implant administration, inter-rater reliability verification, and operational oversight of clinical and surgical quality improvement programs) is collected. The NSO employs well established and secure methods of collecting data from established VA sources, as well as secure sharing with VA National Data Systems for research data use on a secure OIT server in the VINCI environment. The NSO relies on data quality & integrity through VA policies and procedures required for the Veterans health record. VA collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). 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 personal, professional, or financial harm may result for the individuals affected.

Mitigation:
The NSO has implemented restrictions on access to patient PII and PHI stored in the NSO IT System so that only NSO staff who require this information in order to perform their responsibilities to accomplish the mission of the NSO can access it. NSO reports are not available to the general public. Most reports produced by the NSO contain only aggregate metrics (at the National, VISN, or facility level), and access is restricted to key personnel with VHA Surgical Services roles. For those reports that do contain patient level data (including PHI), the surgical record assessment number (which is generated by the VistA system and identifies a unique surgical event for a specific surgical facility) is used in place of patient

identification data. Only PHI that is necessary for proper report interpretation is included. Furthermore, access to patient level data reports is strictly controlled so that only those VA personnel who entered the surgical assessment record data into the VistA system, or who otherwise have a need for patient level data in order to perform their responsibilities, have permission to access these reports. The NSO maintains records for each surgical facility of which personnel need patient level data access and continuously updates these records with ongoing personnel changes. For research data, the VA National Data Systems monitors VA investigator IRB approvals and provides data on a secure server in the VINCI environment which restricts data to use on the server. VA Area Boundary 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. The area 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.

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 the National Surgery Office IT System is to support the NSO in performing its mission of promoting and ensuring the delivery of high quality, efficient, and Veteran-centric surgical care and services, as well as providing operational oversight of clinical and quality improvement activities and to promote research for publications in peer reviewed medical journals.

In relation to VASQIP, surgical data is utilized to monitor and report risk-adjusted surgical outcomes and unadjusted mortality for surgical procedures performed at VA medical centers, across the facility and for each surgical specialty, on a quarterly and rolling 12-month basis with the objective of evaluating the quality of VHA surgical programs and for ongoing improvements to promote Veteran health care. The VASQIP Executive Board utilizes the data from the VASQIP components to provide oversight on quality

assurance activities and review high-outlier Level of Concern metrics which trigger quality assurance site visits. The NSO produces an Annual Surgery Report which provides an overview of Fiscal Year VHA Surgery Program Data for VHA leadership and VHA Program Office reference from a national and regional perspective. Furthermore, these data and analysis result in a NSO Quarterly Report for each VHA surgical program facility which includes chapters covering Outcomes, Quality, Safety, Access, Productivity, Satisfaction, OR Efficiency, and Policy Compliance, and includes facility and VISN level displays of quarterly and rolling 12-month analyses. Additionally, myriad analyses are requested of the NSO on an ad hoc basis by other VHA Program Offices to promote Veteran access to care and quality assurance activities. Finally, these data and analyses are utilized for manuscript preparation for submission to peer reviewed medical journals.

Furthermore, the NSO provides tools to support patient care activities, including Critical Incident Tracking Notification alert system; a patient mortality and morbidity preoperative Risk Calculator; the Invasive Procedure Complexity & CPT Lookup tool to assist with policy compliance and provide operative times; and an NSO Data Viewer that generates a myriad of facility-level and patient-level reports for surgical cases at a single medical center. Additionally, the NSO provides data-driven tools and templates to VHA surgical program facilities and VISN facility workgroups for quality assurance activities and strategic planning initiatives. System information may also be analyzed to perform ad hoc analyses to answer questions related to surgical case volume, outcomes, and patient care under the Freedom of Information Act (FOIA) and from congressional offices such as OSC, OMI, OIG, SVAC, and HVAC. Moreover, the NSO IT System provides aggregated surgical data analysis quarterly to other VHA Program Offices to support the mission of each office, including: IPEC, VSSC, Clinical Inventory, OAA, and QSV. In VA facilities where concern over data quality exists, the NSO manages an Inter-Rater Reliability program to promote quality assurance of the Veteran health record information.

In relation to TRACER, transplant patient clinical characteristics, referral, cost, and reimbursement data is used by Transplant Coordinators and transplant program administrators at VA referring hospitals and VA Transplant Centers for oversight of the transplant referral and patient care process, as well as by the NSO for analysis and reporting on program effectiveness, costs, and for preparing financial distribution to reimburse programs for services and expenses. NSO also utilizes the data from TRACER to produce a national Transplant Quarterly Report for all VA Transplant Centers, perform analyses for manuscript writing, as well as for input to the NSO Annual and Quarterly Reports to promote the care of Veterans requiring transplant services. System information may also be analyzed to perform ad hoc analyses to answer questions related to surgical case volume, outcomes, and patient care under the Freedom of Information Action (FOIA) and from congressional offices such as OSC, OMI, OIG, SVAC, and HVAC.

In relation to the MCAD Tracker component, patient clinical characteristics and device implant data is used to provide MCAD health care coordinators with oversight of device implant and reimbursement oversight. The NSO utilizes this data source for the fiscal management of device implant reimbursement and surgical procedure volume tracking.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring,

reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Tools used to analyze the data within the NSO IT System are SAS, R, SQL Server Management Studio, and Power BI. Results are multiple standardized reports, analytics for manuscript writing, and ad hoc analyses for special requests. Data analysis creates estimated mortality and morbidity risk measures for each VASQIP assessed surgical event received by the NSO from the VistA system. These measures are expressed as the share of total expected risk assigned to a specific surgical event, based on patient and surgical factors in effect at the time of surgery. To obtain accurate risk measure calculations, the NSO creates numerous derived variables covering information about patients from the original VistA input data. For example, input laboratory reading variables typically are transformed into true/false indicators, based on whether their values exceed specified limits, so that they can be used as input to risk modeling formulas. The exact type and number of these derived variables changes from quarter to quarter as the risk models are updated and refined. Another derived measure created by the NSO is the 30-Day Death true/false indicator, regarding whether the patient died within 30 days of surgery. All derived measures are placed in the NSO IT System surgical records obtained from VistA data downloads. No derived measures are placed in any VistA system patient record. Patient mortality and morbidity risk measures, as well as the 30-Day Death indicator, are included in NSO VASQIP reports, but only as surgical case information. All derived measures are intended solely for evaluation of VA facility surgical program quality/performance and have no connection with any action taken for or against any patient.

In relation to TRACER, the NSO creates numerous derived variables covering information about patients from the original referral input data. These derived variables include indicators of referral timeliness and outcome. All derived measures are intended solely for evaluation of VA Transplant Center quality and performance and have no connection with any action taken for or against any patient.

In relation to the MCAD Tracker and IRR Program, the NSO IT System creates no estimated or derived measures.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

VA has processes to protect information at rest or in storage that the NSO IT System implements, which include, but are not limited to the VA approved encryption such as FIPS 140-3 or current version, Transparent Data Encryption (TDE), virtual disk and volume encryption, file/folder encryption, Intrusion Detection and Protection Systems (IDPS), firewalls rulesets, endpoint security to scan for malware and

other threats to confidentiality and integrity, physical and logical access control mechanisms, and change control processes.

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

Fortify Scan rules have been applied which require that the SSN column be renamed to an unfamiliar name that does not contain the words "Social", "Security", "Number" or "SSN".

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

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Data within the NSO IT System database is restricted to personnel of the National Surgery Office. Access is permission controlled, restricted to a small number of office staff with user authentication via VHA GAL user recognition. E-tokens and elevated permissions (e-pas) are required for particular components of the system for database management and configurations, which is closely governed by OIT. Field personnel access is restricted per location and verification of the Key Personnel role they are required to fulfill to access facility-level surgical data for their own facility/VISN.

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

Yes, the NSO reports generated from the NSO IT System that are deemed sensitive are restricted to key personnel at the surgical program facilities, VISN offices, and VA Central Office who are pre-identified by name and require user authentication via VHA Global Address Lookup (GAL) user recognition. FieldComm web requests document access submissions.

2.4c Does access require manager approval?

Yes, for key personnel, local management must approve the request and the request must be submitted to the NSO for final approval. NSO reports that contain PII are restricted to key personnel positions within each VHA surgical program facility who are pre-identified by name, and user authentication via VHA GAL user recognition is required. The transplant-specific data portal with PII is restricted to clinical care providers of the transplant patient and are restricted to key personnel within the treating facility; access to these records require user authentication via VHA GAL with key personnel who are pre-identified by name; local management must approve the request and NSO locally assigned administrators assign personnel with access privileges to their specific location.

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

Yes, the NSO IT System employs the use of event logs for all transactions.

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

The System owner, Developers, System Administrators, NSO PA Team. VHA employees and contractors are required to complete annual confidentiality and privacy trainings and Rules of Behavior verification. Information within the NSO IT System for quality improvement activities are confidential and privileged under the provisions of 38 USC 5705 which protects it from disclosure to anyone without authorization; statute provides for fines up to $20,000 for unauthorized disclosures.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Patient case records related to surgical procedures are retained including those described in Section 1.1 for all NSO IT System components: VASQIP, IRR, TRACER, MCAD Tracker, and NSOSystems.

Patient name, SSN, Date of Birth, Date of Death, Dates related to Surgery Events, Mailing Address, Zip code, Phone number, Email address, Race/Ethnicity

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

National Surgery Office IT System follows VA Records Management Protocol and maintains an active Records Disposition Authority with the National Archives & Records Administration as well as a detailed Service Records Inventory and File Plan. Referencing Disposition #DAA-0015-2016-0006/001—0003 and /0005-007, information retention is 20 years.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

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

General Records Schedule, 5.2, item 020. grs-trs34-sch-only.pdf (archives.gov)

3.4 What are the procedures for the elimination or transfer of SPI?

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

All records within the NSO IT System are electronic and will be purged and ultimately eliminated by the hosting OIT Regional office, per Records Disposition Authority Records Schedule #DAA-0015-2016-0006. Each applicable component of the NSO IT System has retention period to destroy at 20 years after cutoff date and includes the following system databases: Mechanical Circulatory Assist Device (MCAD) Tracker; Transplant Referral and Cost Evaluation/Reimbursement (TRACER); Continuous Improvement in Cardiac Surgery Program (CISCP) Database; National Quality Improvement Program (NSQIP); VA Surgical Quality Improvement Program (VASQIP). Details are maintained in the RCS-10 publication: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

Yes, the NSO IT System uses techniques to minimize the risk to privacy of using PII for testing, training, or research. For trainings, "dummy" test patients are entered into the system rather than displaying real patient II, so no PII is accessible or viewable to trainees. For research, NSO follows minimally necessary standards put forth in VHA Handbook 1200.12, including restriction of accessing patient SSN or PHI data variables for IRB and R&D-approved research analyses. Research datasets are shared through the VA National Data System VSSC's VINCI workspace - a secure, virtual computing environment that provides resources and tools necessary to conduct studies and analyze data.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk:
The data within the NSO IT System is stored in an OIT Regional Data Warehouse and is protected on secure socket layer server technology, thereby reducing risk to privacy breach. There is a risk that the information maintained could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation:
The NSO IT System only retains information necessary to fulfill its purpose, performing longitudinal analysis and reporting up to the number of years of retention. The data within the NSO IT System is stored in an OIT Regional Data Warehouse and is protected on secure socket layer server technology. Data reports are restricted to the intended audience, utilizing user-authentication for access, aligned with the VA medical facility and specific names of VA persons within the key role positions.
To mitigate the risk posed by information retention, National Surgery Office adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The National Surgery Office ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the area to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Received from:			
Corporate Data Warehouse (CDW): Surgery Domain; and Master Veteran Index	To obtain required input data not available in VistA for operational oversight of clinical and surgical quality improvement programs and to provide monitoring of surgery case volumes for evaluation of access management. To obtain verification of patient mortality status and date of death.	Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III) contained in CDW preoperative, intra-operative, postoperative, hospitalization, discharge and readmission records. Completed OR cases, including CDW unique patient identifier, date of surgery, surgical specialty; date of death.	Electronically pulled from CDW through SSMS and SAS. Automated SSIS job that extracts a subset of the CDWWork Surgery Domain on a daily basis.
VistA	To obtain required input data for surgical risk analysis, surgical risk model development/ maintenance, risk-adjusted surgical outcomes/unadjusted mortality reporting, and operational oversight of clinical and surgical quality improvement programs.	PII, PHI, and III primarily from the VistA Surgical Package, as well as VistA clinical, diagnostic, laboratory, Current Procedural Terminology (CPT) code, and demographic data sources.	Electronically pulled through SFTP and Mailman messages from VistA (cardiac) that is compiled in the Surgery Risk Assessment (SRA) database in Hines VAMC OIT (non-cardiac).
VA Office of Academic Affiliations (OAA)	To obtain number of resident positions by division and surgical specialty.	Counts of residents (no PII/PHI)	Excel workbook distributed via email
VA Inpatient Evaluation Center (IPEC)	To obtain acute care and ICU Surgical Mortality Ratios and unadjusted rates.	Rates of adjusted and unadjusted mortality at each surgical program facility (no PII/PHI)	SAS dataset distributed via shared folder on secure server

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
VHA Support Service Center (VSSC)	To obtain information from the Surgical Cases Report, NUMI results, and clinical access and appointment results.	Case counts, access, and appointments availability (no PII/PHI)	Pulled from VSSC online reports
Managerial Cost Accounting Office (MCAO)	To obtain surgical provider staff cost and productivity information	Surgical provider staff total labor cost amounts and productivity metrics (no PII/PHI)	SSRS report pulled from the MCAO website
VHA Office of Quality & Patient Safety	To obtain surgical inpatient satisfaction results	Patient satisfaction scores (no PII/PHI)	Excel workbooks downloaded from the Survey of Healthcare Experience of Patients (SHEP) website
National Center for Organization Development (NCOD)	To obtain surgical staff satisfaction results from the all Employee Survey	Staff satisfaction scores (no PII/PHI)	SAS dataset distributed via e-mail
Shared with:			
VA National Data Systems (NDS)	To provide data to authorized VA researchers for surgical research purposes.	PII, PHI, III from the VASQIP Cardiac and Non-Cardiac Variable checklist, that includes information on the patient's demographic, surgical program info, pre/post op info, and other related surgical info, contained in NSO surgical assessment data extracted from VistA	Electronically uploaded to NDS for the VINCI server environment using SQL as either SAS files or SQL table
VA Inpatient Evaluation Center (IPEC)	To provide Division-level OE ratios from the NSO Quarterly Report	Observed (O) to Expected (E) mortality ratios for each facility (no PII/PHI)	SAS datasets distributed via shared folder on secure server
VHA Support Service Center (VSSC)	To provide a metric for the Network Director Performance Plan	Results (indicators only) for a select number of adverse surgical events for each facility (no PII/PHI)	Excel workbook updated on a VSSC website

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Clinical Inventory	To provide surgical procedure case counts by division and specialty category, and the list of Specialty Surgical Programs by division	Case counts by procedure type and facility surgical specialty program indicators (no PII/PHI)	Excel workbooks distributed via e-mail
VA Office of Academic Affiliations (OAA)	To provide surgical procedure case counts by surgical complexity, surgical specialty, division, and level of resident supervision	Case counts, complexity levels, surgical specialty, and resident supervision (no PII/PHI)	Excel workbook distributed via e-mail
VA Office of Community Care (OCC)	TRACER_database	PII, PHI, and III. SSN, Patient name, Referral date, Requested Organ, Requested location, Review date, Review disposition, Evaluation date, Evaluation disposition, Listing date, Transplant date, Transplanted Organ	Electronically pulled from TRACER through SQL Server Management Studio (outgoing)
Assistant Under Secretaries for Health for Clinical Services and for Operations	To provide internal operational updates on surgical case counts, access, and safety reporting for quality assurance activities and monitoring	Case counts, outcomes, complexity levels, access metrics, safety indicators sometimes including PII	Excel workbook distributed via encrypted email
Office of Productivity, Efficiency and Staffing (OPES)	To provide a current count of equipped Operating Rooms for each facility so they can match for operational efficiency and access	Number of Equipped ORs by facility	Excel workbook distributed via encrypted email
National Program Office for Sterile Processing (NPOSP)	To provide the total count nationally of surgical cases cancelled due to	Total number of cases cancelled and as a percentage of total scheduled surgical cases (rolling year)	Text statement sent via encrypted email

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

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

In relation to the VASQIP component, although most reports produced by the NSO IT System for distribution within the VA contain only aggregate measures, some of them do contain patient level data (including PHI): The NSO IT System provides disclosure of surgical assessment status in the form of a "VA Surgical Quality Improvement Program Case Assessment Status report" (Status Report), which contains PHI, as feedback on data completeness and accuracy issues; and the NSO Data Viewer provides a facility with a view of their surgical patient case information. For the IRR component, PHI is included in the report, but there is no distribution throughout the VA.

In relation to the TRACER component, most reports produced by the NSO IT System for distribution within the VA contain PII and PHI.

In relation to the MCAD Tracker component, reports produced by the NSO IT System for distribution within the VA contain PII and PHI. The internal sharing of data is necessary individuals to receive benefits at the NSO IT System.

Mitigation:

In relation to the VASQIP component, for those NSO IT System reports shared within the VA that do contain patient level data (including PHI), the surgical record assessment number (which is generated by the VistA system and identifies a unique surgical event for a specific surgical facility) is used in place of patient identification data. Only PHI that is necessary for proper report interpretation is included. Furthermore, access to patient level data reports is strictly controlled so that only those VA personnel who entered the surgical assessment record data into the VistA system or those who otherwise have a need for patient level data in order to perform their responsibilities, have permission to access these reports. Status Reports have access restricted to only the surgical facility personnel specifically responsible for entering surgical data into the VistA system. For the IRR component, only PHI that is necessary for proper assessment interpretation is included. Furthermore, access to these assessments is strictly controlled so that only NSO staff and the participating surgical assessment team (Surgical Quality Nurse, OR Manager, Chief of Surgery, Chief of Staff; Chief Medical Officer, Quality Management Officer, VCSC, VLSN,

VISN SICC Clinical Lead, and VISN SICC HSS-Admin) have permission to access these assessments. The NSO maintains records for each VHA surgical facility of which personnel need access to these reports and continuously updates these records in response to ongoing personnel changes.

In relation to the TRACER component, only PII/PHI that is necessary for proper dashboard/report interpretation is included. Furthermore, access to these dashboards/reports is strictly controlled so that only NSO staff, Transplant Coordinators, and transplant program administrators (who have a need for this data in order to perform their responsibilities) have permission to access these reports. The NSO maintains records for all parties involved with the Transplant Coordinator and transplant program administrator functions and continuously updates these records in response to ongoing personnel changes.

In relation to the MCAD Tracker component, only PII/PHI that is necessary for proper dashboard/report interpretation is included. Furthermore, access to these dashboards/reports is strictly controlled so that only NSO staff and MCAD Coordinators (who have a need for this data in order to perform their responsibilities) have permission to access these reports. The NSO maintains records for all parties involved with the MCAD Coordinator function and continuously updates these records in response to ongoing personnel changes.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Not applicable; information from the NSO IT System is not shared outside of the VA.

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

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

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Data within the NSO IT System is collected as part of the Veteran patient consent process covered under the Notice of Privacy Practice (NOPP), as the NSO IT Systems is a compilation of medical record data. The NOPP protocol is described below.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP is given out when the Veteran enrolls; and when updates are made to the NOPP, copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis.

There is one System of Record Notices (SORNs):
SORN 121VA10 - 'National Patient Databases-VA", which is published in the Federal Register and online: 2023-07638.pdf (govinfo.gov)

This Privacy Impact Assessment (PIA) also serves as notice. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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.

The Veterans' Health Administration (VHA) facilities request only information necessary to administer benefits to Veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

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. 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 where required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk:
There is a risk that an individual may not understand that information is being collected or maintained about them.

Mitigation:
This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. 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 (SORNs) and Privacy Impact Assessments (PIA) available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The VHA National Surgery Office data from the NSO IT System may be requested under the FOIA process and released through an intermediary, the VA FOIA Service, who ensures that VA policies comply with Federal regulatory requirements and legislative mandates. If any Veteran patient information is found to be inaccurate, the correction request is not applicable for the NSO IT System, but rather is directed to the local VA facility to correct within the patient source record (e.g., within VistA), as described below:

There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

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.

If any Veteran patient information is found to be inaccurate, the correction request is not applicable for the NSO IT System but rather is directed to the local VA facility to correct within the patient source record (e.g., within VistA), as described below:

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

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

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.

Procedures for correcting an individual's information is not applicable to the NSO IT System, but is a procedure managed by VA Directive 6300 "Records and Information Management" and is detailed in the Notice of Privacy Practice, as described below:

Veterans are informed of the amendment process by many resources to include the 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 (PO) 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

Information can also be obtained by contacting the facility ROI office.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Redress is not applicable to the NSO IT System.

For the patient record amendment process, Veterans and individuals should use the formal redress procedures addressed above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk:
There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veterans receive.

Mitigation:
As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records. The VHA Release of Information (ROI) offices at facilities are 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 health records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy and Release of Information Directive 1605.01 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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

The user must exist in active directory and be assigned application roles that are granted by the NSO office for access to controlled applications under the ATO.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

The NSO IT System data content is only accessible to the VA clinical care team and restricted to the content aligned with their VA facility patients. The access control procedure requires user authentication to the VA Network using their current PIV card (Windows Integrated Authentication), followed by access to a URL-based Microsoft ASP.NET Web application, which is then further authenticated using Microsoft Identity (checking backend services from VA Active Directory) to authenticate users.

The NSO IT System data stores are only accessible by the staff of the National Surgery Office who perform the program analytics, statistical evaluations, and clinical and operational oversight of this national program office. The host servers are configured with Secure Socket Layer technology. Access to the databases requires multiple access control procedural steps including user authenticates to the VA Network using active VA PIV card, is then authenticated by Active Directory Integrated Windows Authentication, and requires a non-email "zero account" to ensure an additional layer of user recognition and system protection.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Roles are used to determine access to an application and assigned to users, depending on the request and requirements. Based on roles given, users may have 'read-only' access, while others, such as admins, may be permitted to make certain changes to the information.

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.

Two on-site NSO contracted staff regularly access and assist in the maintenance of the programs that pull, report and store data collected. Contracted staff must have Privacy and Confidentiality training, abide by the Rules of Behavior, and be approved through the contracting process to be allowed access to VA and NSO systems as well as access to PHI/PII.

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.

Mandatory annual (or other identified periodic interval) VA, VHA, Regional and facility privacy and HIPAA training is required, including but not limited to "VA Privacy and Information Security Awareness and Rules of Behavior," and "Privacy and HIPAA Training."

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

A one-year ATO was granted 06 Jan 2023.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

N/A

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.09.27 16:08:45 -04'00'

Privacy Officer, Nancy Katz-Johnson

SHARON GAINEY

Digitally signed by SHARON GAINEY
Date: 2023.09.27 14:55:11 -05'00'

Information System Security Officer, Sharon Gainey

MARK A. WILSON 247245

Digitally signed by MARK A. WILSON 247245
Date: 2023.10.03 12:56:27 -04'00'

Information System Owner, Mark Wilson

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).

VHA Notice of Privacy Practices

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices