SWOG CANCER RESEARCH NETWORK

System Security Verification
SWOG Statistics and Data Management Center

This document describes how the SWOG Cancer Research Network's Statistics and Data Management Center (SDMC) manages the transmission, processing, storage and maintenance of data submitted by all SWOG participating institutions, including VA Veterans Health Administration (VHA) facilities managed by the Department of Veterans Affairs (VA) and DoD Military Health System (MHS) facilities managed by the US Department of Defense (DoD).

The SWOG SDMC securely maintains research data following best practice policies and procedures. SWOG Policy Memorandum No. 31 (April 2018) describes SWOG's acknowledgement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule as it relates to data used in research. SWOG maintains certification and accreditation for compliance with the security framework required under the Federal Information Security Management Act (FISMA) of 2002 and the Federal Information Security Modernization Act of 2014, adhering to standards promoted by the National Institute of Standards and Technology (NIST). A current FISMA certification and accreditation is posted on the SWOG website – www.swog.org.

1. ORGANIZATION INFORMATION

SWOG Organizations. Organizations involved in providing, handling, accessing, processing and analyzing, and storing research data include the following entities:

Group Chair's Office:
Oregon Health & Science University (OHSU) hosts the headquarters for SWOG, a National Cancer Institute-supported cancer clinical trials cooperative group. The SWOG Group Chair's Office (GCO) at OHSU provides leadership from its offices located at 3181 SW Sam Jackson Park Road; MC: L586; OHSU; Portland, OR 97239.

Additional GCO leadership and support is provided from The Hope Foundation, located at 24 Frank Lloyd Wright Drive, Ann Arbor, Michigan 48106.

Operations Office:
Operational support is provided from the Operation's Office, located at 4201 Medical Dr., Ste. 250; San Antonio, TX 78229-5631.

Statistics and Data Management Center:
Fred Hutchinson Cancer Research Center (Fred Hutch), a national cancer research institute, based in Seattle, WA, houses the SWOG statistical component of the SDMC. FRED HUTCH is located at 1100 Fairview Ave. N. (P.O. Box 19024); Seattle, WA 98109.

Cancer Research And Biostatistics (CRAB), a non-profit research organization, houses the SWOG data management component of the SDMC where all research data are collected, stored and processed. CRAB is located at 1505 Westlake Ave N, STE 750; Seattle, WA 98109-6244.

Work Locations. The Primary Work Location (PWL) is the CRAB facility where all data are maintained. An Alternate Work Location (AWL) is the FRED HUTCH facility. Biostatisticians at the AWL access research data at CRAB via secure systems described herein.

2. SECURITY PRACTICES

SWOG SDMC does not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.

SWOG SDMC uses appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

SWOG SDMC will report to a participating institution(s) any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

SWOG SDMC ensures that any agent or third party, to whom it provides Protected Health Information received from, or created or received by the **SWOG SDMC** on behalf of the any participating institution, agrees to the same restrictions and conditions that apply through this Agreement to **SWOG SDMC** with respect to such information.

SWOG SDMC will make available for on-site review in a timely manner internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by **SWOG SDMC** on behalf of any participating institution.

3. SYSTEM SECURITY

Information Exchange Security. Information transmitted over the Internet using SWOG's electronic data capture (EDC) CRA Workbench system is protected using Transport Layer Security (TLS). The electronic data exchange is compliant with NIST SP 800-52 Rev. 2 (August 2019) which designates the use of TLS 1.2 for the transmission of qualifying federal data with migration to TLS 1.3 by January 1, 2024. Additionally, SWOG systems follow the Federal Information Processing Standards (FIPS) Publication 140-3 (May 2019). The scope and requirement for use of only 140-3 approved encryption algorithms also extends to applications that process the data, in this case the SWOG electronic data capture system upon which older studies continue to be hosted. The connection at the **SWOG SDMC** is located within controlled access facilities, secured and monitored 24 hours a day. All approved user access to data is validated and authenticated through both operating system and application security mechanisms.

Since August, 2012, new trials are implemented within Medidata Rave®, a commercial EDC system purchased via the National Cancer Institute (NCI). Medidata has agreed to ensure that Rave-based trials processed through SWOG Rave EDC servers utilize TLS 1.2 and compliant encryption methods for all data submissions. The Rave authentication portal, called iMedidata, which must be available to all Medidata clients, also utilizes TLS 1.2. Rave trials are hosted at Medidata's secure data center.

Computer/Network Technical Controls. Data protection at the SDMC includes the use of network firewalls and intrusion prevention/detection systems. Computer operating systems on servers and workstations are maintained with the latest patches and security updates following the SDMC patch management procedures. Anti-virus and anti-spyware is installed and automatically updated on workstations and servers.

Workstation Inactivity. Logon sessions have enforced password protected screen savers that lock the systems after 20 minutes of inactivity. Both failed and successful user authentication attempts are centrally logged. Failed logon attempts are formally reviewed as part of a daily checklist procedure.

Trusted Behavior Expectations. SWOG and participating institutions are expected to protect protected health information in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710), and HIPAA. The **SWOG SDMC**, while not a covered entity under HIPAA, follows best practices for the protection of research data, including personal identifying information.

Formal Security Policy. Policies or directives that govern the protection of the data are the **SWOG SDMC PWL's** Network Security Protection procedures.

Incident Reporting. The person discovering a security incident will report it in accordance with its incident reporting procedures. In the case of **SWOG SDMC**, any security incident will be reported to the point of contact on file with **SWOG SDMC** or the principal investigator listed within the Purchase Service Agreement between SWOG and the Principal Investigator so that the incident can be reported to the Research Office or designated department at the participating institution for report and action. No system data breaches have occurred at the **SWOG SDMC**.

Audit Trail Responsibilities. SWOG and participating institutions are responsible for auditing application processes and user activities involving the interconnection with sufficient granularity to allow successful investigation and possible prosecution of wrongdoers. Database and web server activities at the **SWOG SDMC** are logged, including event type, date and time of event, user and workstation identification, success or failure of access attempts, as well as security actions taken by Information Technology (IT) staff. Audit logs at the **SWOG SDMC** are retained for at least one (1) year.

Event Log Responsibilities. Event log capture and monitoring has been implemented on all production servers at the **SWOG SDMC**. Automated real-time log monitoring is in effect 24 x 7, with email and page alerts sent to IT staff when appropriate, based on the severity of the issue. In addition, all log reports are reviewed by staff daily. Database transaction logs are backed up regularly throughout the day and are reviewed when necessary to investigate or remediate.

Conduct Security Reviews. SWOG and participating institutions should review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure they are operating properly and are providing appropriate levels of protection. Annual review is performed at the **SWOG SDMC PWL**.

Manage User Profiles. SWOG and participating institutions should actively manage user access rights. If a user resigns or changes job responsibilities, the appropriate organization should update the user's access rights to prevent access to data or information that is no longer appropriate. Procedures for investigating and revoking access rights to users who do not actively access the interconnection over a specific period of time should be established.

Physical Security. Data are stored on server and disk storage systems in the **SWOG SDMC PWL** data center. The data center and equipment and media storage rooms are secured behind locked doors. Access is restricted to authorized staff and controlled via an electronic keycard system. Physical security to the office suite is restricted and managed through an electronic keycard system. Elevators require keycard access outside normal business hours. Procedures are in place to track visitor arrivals and departures; all visitors are escorted by authorized staff at all times. All entry points into the office suite are monitored through video surveillance. The data center and equipment and media storage rooms have additional video surveillance within the rooms.

Network Security. Access to network resources is secured through Microsoft Windows Active Directory technology. Active Directory authentication is used to control access to network services. Security policies are enforced through Windows Active Directory group policy and applied to users, workstations and servers. All users are required to use strong, complex passwords (those with a combination of lower- and upper-case alphabetic characters, numbers and special characters).

Data Center Disaster Mitigation. Servers and network appliances are housed in the data center at the **SWOG SDMC PWL** which includes a self-contained HVAC (heating, ventilation, and air conditioning) system with redundant fans and pumps and a UPS (uninterruptible power supply) which delivers conditioned power to racks of servers and includes enough capacity to provide power for up to one hour during short power outages and to allow for the safe shut down of systems during a longer outage. The fire suppression and safety systems include an automatic pre-action dry pipe system where sprinkler pipes are devoid of water until needed. The HVAC, UPS, and fire suppression systems are under regular preventative maintenance plans by qualified facilities' vendors.

Remote Access. **SWOG SDMC** staff access resources remotely via Citrix XenApp or Microsoft Remote Desktop Gateway connectivity. Communication and data are secured using 2048-bit TLS encryption and Microsoft Active Directory user network-level authentication. Additionally, a second factor of authentication is performed using RSA SecurID token-based technology or by Microsoft's Azure Multi-Factor Authentication service, depending on the remote connection type. Data that are uploaded via CRAB's Secure File Transfer Protocol (sFTP) server uses Secure Shell File Transfer Protocol (SSH) or Transport Layer Security (TLS) to encrypt and secure data in transit.

Paper Format. Data printed to paper format are protected to prevent unauthorized access through the use of signed confidentiality agreements, locking file cabinets and locked shredding bins.

Training and Awareness. All **SWOG SDMC** employees are required to undergo Good Clinical Practices (GCP) and Human Subjects Protection training. Staff members at the **SWOG SDMC PWL** location are required to undergo Security Awareness Training and to sign agreements governing professional conduct, conflict of interest, code of conduct, and access to and use of computing equipment and research data.

4. DATA BACKUP/MEDIA PROTECTION

Data Backup. Disaster recovery, data backup and archival processes are based on best practices in data protection with particular emphasis on regulatory requirements. Systems administrators routinely review and compare current practices with existing policies and procedures. Updates to policies, procedures, and training are incorporated as appropriate. Tape library systems are used for nightly data backups as well as for data recovery and permanent archiving. All data written to tape is encrypted. Current technology uses state-of-the-art Linear Tape Open (LTO) tape types while legacy tape systems are retained to read older media.

Data Backup Storage. Tapes are initially written in the secure data center and then moved to a fireproof media cabinet in a secure, restricted media storage room. The most recent backup tapes are stored in a fireproof safe. The room is environmentally controlled and secured with keycard access.

Off-site Storage. Data backup tapes are transferred to off-site secure storage by secure messenger in a tamper-evident sealed case. The secure data storage vendor's data vault provides protection from fire, extremes of temperature and humidity with a Firelock media vault, described as the largest such vault in North America. The media vault provides a U.L. 72 Class 125 rating that is recognized as the most stringent fire protection standard for data backup media in the world. Security is controlled through card key access. Double doors provide secure entry with an inner door closer that is linked to the automatic closer on the outer door so they close in unison. Only authorized **SWOG SDMC** staff may request data. These requests are made through a secure online application which also provides inventory management and control.

Media Sanitization. Disposal, purging, and destruction of hard copy and electronic forms of Protected Health Information is paramount. Competent data destruction services are used to ensure that no data can be recovered from obsolete electronic media. Magnetic-based storage media at the **SWOG SDMC** is sanitized with a minimum of three passes of a U.S. Department of Defense approved disk sanitation method. Magnetic-based storage media is then stored securely until it can be sent with non-magnetic media to an offsite storage media destruction service which provides a certificate of destruction document upon completion.

Data Storage/Disposal. **SWOG SDMC** stores personal identifying information separately from other research data and access is restricted and controlled. Disposal of media on which these data are stored follows **SWOG SDMC**’s media sanitization procedures.

Data Retirement. Most data used in SWOG studies are retained indefinitely. If it is determined that data are not to be retained, that data are removed from servers following a plan as defined in **SWOG SDMC** Research Data Destruction procedures.

5. INTERCONNECTING INFORMATION SYSTEMS

General Information/Data Description. An interconnection between workstations with Internet browsers exists between the participating institution and both the SWOG web-based CRA Workbench and the Medidata Rave® system. The purpose of the interconnection is to deliver research data to **SWOG SDMC**’s Data Analysis Department and to deliver confirmations and reports to workstations with Internet browsers at the participating institutions’ Research Office.

Services Offered. Services include data exchange whereby data are submitted via workstations with Internet browsers at the participating institution through the SWOG web-based CRA Workbench and the Medidata Rave® system, both hosted on secure Internet electronic data capture (EDC) applications.

Sensitivity Categorization. The sensitivity categorization of data exchanged between the participating institution and **SWOG SDMC** based on FIPS 199, *Sensitivity Categorization of Federal Systems*, and the guidance in NIST SP 800-60 is defined as Moderate to Low.

6. DATA FLOW

Receipt of Data. Data will be entered by the user via the SWOG EDC, either through the SWOG CRA Workbench or Medidata Rave®. Source documents required by the study (e.g., pathology reports) will be uploaded directly to SWOG via the EDC or, rarely, faxed via an internal data processing program at the **SWOG SDMC**. Safeguards include the following:

a. SWOG systems utilize the NCI required CTEP IAM (Identity and Access Management) username and password for authentication. All users are required to use strong, complex passwords with a combination of lower and upper case alphabetic characters, numbers and special characters. CTEP IDs are authenticated against a Cancer Trials Support Unit (CTSU) user database via a Web service.

b. SWOG members are also assigned a unique roster ID number with a temporary password the user must change upon receipt. All users are required to use strong, complex passwords with a combination of lower and upper case alphabetic characters, numbers and special characters.

c. For CTEP IAM and SWOG Roster IDs, permissions are role-based, application-specific and managed by the local Web User Administrator appointed at each site.

d. Logon sessions have enforced password protected screen savers that lock the system after 20 minutes of inactivity.

e. Data submission via the EDC will only display the assigned SWOG patient number, study number, patient initials, and additional study data as approved. It will be the responsibility of the site to provide SWOG patient number, study number, and patient initials on all source documents and to redact non-study data prior to submission.

Dissemination of Data. Data access is restricted to authorized users. Data submitted electronically are stored in a patient-specific electronic chart. Source documents submitted by fax are routed to the electronic chart by a SWOG Data Control Technician. Static images in the electronic chart are reviewed by SWOG Data Coordinators and derived codes pertaining to eligibility, treatment, response, and adverse events are entered in the SWOG database. Safeguards include the following:

a. SWOG personnel are required to sign a confidentiality agreement which restricts each individual from disclosing any confidential information including all information or data which would permit the identification of individual study subjects or participants.

b. SWOG study-specific informed consent documents allow for the sharing of patient-specific data. SWOG Policy No. 43 covers Requests for Patient Data from SWOG Studies. Any external requests for patient-level data outside the SDMC will be evaluated at the SDMC for appropriateness and feasibility. Further review is performed by the SWOG executive committee to assess resources required to conduct the data sharing. Once approved, a data use agreement (DUA) is executed between the investigator and SWOG with specifications including data and services, compensation and expenses, use and publication, indemnification, and other provisions. No PHI is included in any outgoing data sets, and a pseudo-patient ID is used to identify each patient record so no link can be made by an outside investigator to a patient's clinical record

Disposition of Data. All data stored in the patient-specific electronic chart are retained indefinitely. Once a study has been published, is no longer collecting follow-up and evaluation efforts have ceased, a determination may be made to archive the records but they will not be destroyed or deleted. Any paper copies printed from the electronic chart for auditing purposes will be shred and are not allowed to be stored.

Fax Transmission of Data. Fax submission of data is rare. The only data permissible for fax submission are source documents such as a pathology report. It will be the responsibility of the site to provide patient initials, SWOG patient number and SWOG study number on all source documents, redacting PHI prior to submission.

Voice Transmission of Data. Users may contact the **SWOG SDMC** for questions related to eligibility, expectations and queries on a patient-specific level. However, a caller should never refer to the patient by name or use other PHI when detailing the issue by voice mail. Only initials, SWOG patient number and study number should be used.

7. DATA ACCESS

User Community. **SWOG SDMC** users with access to SWOG data include those with access to the following: data coordinators who review the data and resolve queries; statisticians who analyze the data; network and systems administrators who provide support and backup for the systems; the Oracle database administrator who manages the databases; and application developers who provide programming support.

User Access. Access to the Oracle database used for SWOG clinical trials data are controlled according to the user’s role and job function. Staff members have separate accounts for the network, database, and Web applications. These Oracle accounts are user-based, and are created only for those who need direct access to the database as part of their job function with rights granted in accordance with the required level; of access needed to accomplish project objectives.

Access Termination. **SWOG SDMC** staff members follow SOPs regarding termination of employment. All network and database access is immediately disabled. Staff members who leave the organization surrender their keys, keycards, and wo-factor authentication devices before exiting the building on their last day of work.

User Review. All **SWOG SDMC** users with access to the data received from participating institutions are approved to work in the U.S. as confirmed by Form I-9, Employment Eligibility Verification. All users have undergone a background check and are trained on Professional Conduct and complete Protecting Human Research Participants (PHRP) and Good Clinical Practices training.