SWOG Statistics and Data Management Center
Supported at Cancer Research And Biostatistics

2022-2023
FISMA Compliance Assessment

**Federal Information Security Modernization Act of 2014*

Reviewed October 31, 2022

Covering Security for Systems within the Scope of FISMA 2002 Requirements

Statement of Certification and Accreditation

The undersigned certify that to their knowledge that SWOG Cancer Research Network Statistics and Data Management Center (SDMC) information systems and constituent system-level components located at Cancer Research And Biostatistics (CRAB) and within the purview of FISMA 2014 and the NIST Risk Management Framework (v. 1.1), including the Rave® Electronic Data Capture (EDC) system hosted at Medidata, meet compliance requirements. Based on security certifications of systems and supporting evidence provided in the associated security accreditation package (including current system security plan, security assessment report, and plan of action and milestones), the undersigned have determined that risk to information provided by public and private agencies is acceptable. This is a formal declaration that security controls have been implemented in the information system and that security meets or surpasses levels of acceptable risk. A summary of recommendations for implementation of additional security controls is attached.

This certification and accreditation of the information system will remain in effect through the next renewal period, 4th quarter of 2023, as long as any potential vulnerability reported during continuous monitoring processes do not result in unacceptable risk.

DocuSigned by:
Lisa R. Upshaw
Signer Name: Lisa Upshaw
Signing Reason: I approve this document
Signing Time: 12 December 2022 | 10:38:12 PM PST
452DEF8D0C954257B90DD3445D962AC9

Lisa Upshaw, Director of Quality Compliance

DocuSigned by:
Curt Malloy
Signer Name: Curt Malloy
Signing Reason: I approve this document
Signing Time: 14 December 2022 | 1:57:11 PM PST
46BFFF29F6C04E87A27F5519396D7D61

Curt Malloy, Vice President, Chief Operations Officer

DocuSigned by:
Chris Cook
Signer Name: Chris Cook
Signing Reason: I approve this document
Signing Time: 13 December 2022 | 9:20:18 AM PST
45B82BC752914E8CB08DF526E9D58A6D

Chris Cook, Chief Technology Officer

The complete 2022-2023 FISMA Compliance Assessment is available to SWOG member institutions upon request.

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Certification based upon NIST Risk Management Framework, including in part:

Special Publications
800-52 Rev. 2 (August 2019)
800-53 Rev. 5 (Dec 2020) Security and Privacy Controls for Information Systems and Organizations
800-53B (Oct 2020) Control Baselines for Information Systems and Organizations
800-60, Rev. 1 (Aug. 2008) Guide for Mapping Security Controls

FIPS Publications
140-2 (Dec 2002) Security Requirements for Cryptographic Modules
199 (Feb. 2004) Standards for Security Categorization of Federal Information and Information Systems
200 (March 2006) Minimum Security Requirements for Federal Information and Information Systems

Other NIST Publications and Security Analysis Tools

SUMMARY OF RECOMMENDATIONS

1. Information Security Architecture (PL-8): Current Standard Operating Procedures (SOPs) cover internal systems. We provide due diligence in review of external systems which are evaluated using the same criteria as internal systems. External systems used with federal data are reviewed by the NCI for security compliance. The SWOG SDMC reviews compliance reports for external systems as they are made available.
2. Supply Chain Risk Management Plan (SR-2): SDMC staff are developing a Supply Chain Risk Management Plan that assesses dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, that present an increasing level of risk to an organization. The Supply Chain Risk Management Plan will be implemented prior to the next compliance assessment.
3. Supply Chain Controls and Processes (SR-3): SDMC staff are developing Supply Chain Controls and Processes that include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply Chain Controls and Processes will be implemented prior to the next compliance assessment.