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

2017-2018
FISMA 2002*
Compliance Assessment

*Federal Information Security Management Act of 2002
Reviewed October 5, 2017

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 Statistics and Data Management Center (SDMC) information systems and constituent system-level components located at CRAB and within the purview of FISMA 2002, including the Rave® Electronic Data Capture (EDC) system hosted at Medidata, are in compliance. 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 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 annual renewal period, 4th quarter of 2018, as long as any potential vulnerability reported during continuous monitoring processes do not result in unacceptable risk.

Grace Powell, Regulatory Affairs | Quality Assurance Manager

Curt Malloy, Vice President, Chief Operations Officer

Keith Goodman, Vice President, Chief Technology Officer

Date

Date

Date

The complete 2017-18 FISMA Compliance Assessment is available to SWOG member institutions upon request.

Certification based, in part, upon:
- FIPS Publications 140-2 (May 2001) (Security Requirements for Cryptographic Modules)
- Other NIST Publications and Security Analysis Tools

© 2017 Cancer Research And Biostatistics (CRAB®). All Rights Reserved. CONFIDENTIAL.
SUMMARY OF RECOMMENDATIONS

1. Media Use: SDMC staff utilize iPhone and BlackBerry devices which have been deployed using best practices for security and privacy. An SOP covering mobile support is under development and review. It is recommended that this SOP be completed prior to the next review.

2. Information Security Architecture: Current 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. An SOP will be developed to detail the process in use. It is recommended that this SOP be completed prior to the next review.