SPARCS Security Guidelines for External Requestors

When completed, please return signed document to the SPARCS program using SPARCS Support.

Security Guidelines

The New York State Department of Health (the Department) places a high priority on protecting the data contained within the Statewide Planning and Research Cooperative System (SPARCS) data system.

This document identifies the SPARCS security guidelines that must be adhered to by the recipient(s) of SPARCS data and is applicable to cloud, on-premises, and hybrid environments. The Department reserves the right to request information to confirm compliance with the attested security provisions, and to make updates or changes to these provisions at any time.

Data recipients may periodically be asked to re-attest to the SPARCS Security Guidelines and that the data provisioned is still required for the approved project or use case. Data recipients that fail to maintain compliance or attest may have their permission to SPARCS data rescinded consistent with NYS regulations.

Security Provision
1. Organizations and individuals requesting SPARCS data must at a minimum adhere to NYS Encryption Standard (NYS-S14-007).
2. SPARCS data must be encrypted in transit using Transport Layer Security 1.2 or later. SPARCS data shall remain encrypted at rest using federally approved AES-128 or higher encryption per: NYS Encryption Standard (NYS-S14-007).
3. If a stand-alone system or local workstation is used, it will have an encrypted hard drive, have no access to or from the Internet, exist in a secure location (such as a locked office), be accessible only to authorized individuals, use strong password protection, and be locked after a maximum inactivity period of 15 minutes per NYS Account Management/Access Control (NYS-S14-013).
4. The storage system (cloud or on- premises) will be able to generate an immutable log of unique IDs that access the data, from what location (if available), and the dates and times. This unique ID that accessed SPARCS data must associate with the individuals who access SPARCS data. The logging must show all access to SPARCS data and identify access by both authorized and non-authorized users. Logging must comply with NYS Security Logging (NY S- S14 - 00 5). This audit log will be presented to the Department, within a reasonable time, upon request.
5. Remote connections will occur over a VPN when possible and comply with the NYS Remote Access Standard (NYS-S14-010).

6. SPARCS data shall not be stored on removable media (i.e., CDs, thumb drives, or other external storage devices), unless approved by the Data Governance Committee. If approved, the device will be encrypted using a FIPS-approved algorithm. Refer to NYS Encryption Standard (NYS-S14-007).
7. Using a cloud hosted or third-party software for geocoding is prohibited unless approved by the Data Governance Committee or the SPARCS Program, as applicable.
8. Access to approved minimum necessary SPARCS data may be permitted only upon approval of the user's signed individual affidavit. The SPARCS data may be used solely for the purpose(s) stated in the application.
9. SPARCS data shall not be used, accessed, stored, or disclosed unless approved by the Data Governance Committee or SPARCS Program, as applicable.
10. Upon expiration or rescission of approval, all SPARCS data must be destroyed by an approved process following NYS Sanitization Secure Disposal Standard (NYS-013-003). Acceptable methods for non-recoverable destruction of stored data are physical destruction or forensic wiping. Documentation of the destruction process or extension request is available on the SPARCS Forms Page and must be submitted on a signed affidavit via the SPARCS Support site.
11. Organizations that are unable to meet one or more of these provisions may submit a separate written request for approval of an exception in the form of an attachment to this affidavit; any request for exception(s) to these Security Guidelines must include information on compensating controls. Compensating controls are security and privacy controls implemented in lieu of the baseline controls that provide equivalent or comparable protection for a system or organization.

Data Security

Approved Limited and Identifiable data file users are required to take all necessary precautions to prevent unwarranted invasions of personal privacy resulting from any data analysis or release. Data users may not release any information that could be used, alone or in combination with other reasonably available information, to identify an individual who is the subject of the information. Data users bear full responsibility for breaches or unauthorized disclosures of personal information resulting from the use of SPARCS data.

Security Incident Reporting: If the Project Director or any member of the project team becomes aware of a data security incident (e.g., inadvertent disclosure, system compromise [e.g., ransomware], or other type of breach/disclosure), they must immediately email the SPARCS program at: sparcs.requests@health.ny.gov. The email should include the SPARCS Request Number, the number of years of data involved and outline the nature of the data security incident. The email must include the title, email, and phone number for the organizational representative responsible handling the incident response.

Breaches or other infractions of the SPARCS data use agreements may result in the assessment of penalties against the Project Director, the requesting organization, or both. Penalties may include monetary fines as authorized by Public Health Law Sections 12 and 12- d, rescission of a prior approval to use SPARCS data, and/or a bar on any future use of SPARCS data by the requesting organization as whole.

Change Log

The SPARCS program has made every effort to provide accurate and complete information in these Security Guidelines. Any typographical error is unintentional, and we urge users of this document to bring them to our attention for correction. Edits, deletions, modifications, or changes to areas of this manual will be maintained in a change log and updated versions of the manual will be released.

Version	Date	Updates
1.0	September 2014	• Initial publication
2.0	December 2021	• Updated citations and added links to NYS Standards; revised acknowledgement/signatory section • Added notarization section and glossary
3.0	May 2022	• Revised acknowledgement section to clarify that the Organizational Representative who signs the Organizational Data Use Agreement should also be the signatory on the Security Guidelines
4.0	April 2024	• Revised Provision #4 - Logging • Revised Provision #5 - Linked to the Remote Access Standard Provision #6 - was combined with section #3 • Provision #7 - BYOD Policy reference removed • Data Security Section added • Glossary - BYOD Policy reference removed
4.1	July 2024	• Revised Provision # 9 – Use of Data per DGC or SPARCS program approval • Added provision # 11 – Exceptions/compensating controls • Updated Signature space labels to clarify that signatures are required from the requesting organization's CISO or IT Lead and Organizational Representative
4.2	March 2025	• Updated link to NYS ITS Encryption Standards (NYS-S14-007) • Updated submission instructions
4.3	April 2025	• Removed glossary • Amended attestation requirements

SPARCS Security Guidelines for External Requestors

Acknowledgement

We, _____, the acting or current Chief Information Security Officer (Chief Information Security Officer [CISO]) or lead Information Technology administrator and _____, the Organizational Representative, hereby attest to the following on behalf of (SPARCS Data Requesting Entity) _____.

- The requesting entity shall adhere to the SPARCS security guidelines listed above.
- The New York State Department of Health may request information or audit the requesting entity at any time to ensure compliance with SPARCS security guidelines.

Signatories

_____ _____

CISO or Lead Information Technology Administrative Signature | Date

Signer's Name (please print) _____

Organization _____

Email Address _____

Address _____

Date _____

Organizational Representative Signature _____