The New York State Department of Health, Bureau of All Payer Systems and Informatics places a high priority on protecting the identifiable data elements contained within the Statewide Planning and Research Cooperative (SPARCS) data system.

This document has been prepared to ensure individuals who apply to use SPARCS Data are aware of the security protocol at their organization. An organizational representative must attest to each data protection standard that is in place at their organization by having an IT Tech initial where applicable, then signing the second page of this document.

Initial	Security Provision
	1. SPARCS data is required to be stored on a network server that uses Transport Layer Security 1.1 or later, or another federally recognized encryption protocol to protect data in transit from unauthorized access. The server must be located behind a properly activated firewall, and data must remain encrypted at rest using federally approved AES encryption.
	2. If a network server is unavailable, a stand-alone PC may be used to store SPARCS data. If a stand-alone system 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, be password protected, and have an enabled screensaver set to activate at 5 minutes of inactivity.
	3. The storage system will be able to generate a log of unique IDs that access the data, from what location, and the dates and times. This audit log will be presented to the Department, within a reasonable time, upon request.
	4. All remote connections from offsite locations shall be approved by the Data Governance Committee. Approved remote connections will occur over a VPN and comply with the NYS Encryption Standard (NYS-S14-007), a document describing New York's encryption standards for data in transit.
	5. If using a local workstation to access the data, it will be connected to the network from a secure location, be accessible only to authorized individuals, use password protection, and have an enabled screensaver set to activate at no more than 10 minutes of inactivity.
	6. 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.
	7. Geocoding will not be done in the cloud or with online software programs. All methods and applications used for geocoding will be approved by the Data Governance Committee.
	8. Access to approved SPARCS data will be permitted only upon approval of the user's signed individual affidavit. The user will then be authorized to use that data only and solely for the purpose(s) stated in the application for which the affidavit was submitted.
	9. SPARCS data will not be shared with anyone, in any form, unless described to and approved by the Data Governance Committee. Doing so would cause a breach of security, and subject us to possible penalties.
	10. At the time of expiration (three years after the last year of data is sent), all SPARCS data must be returned, and all copies destroyed by an approved process or authorized vendor. Acceptable methods for non-recoverable destruction of stored data are physical destruction or forensic wiping of the media. Documentation of the destruction process is required. An extension may be requested via email to sparcs.requests@health.ny.gov.

Signature of organizational representative authorized to legally bind the organization that is applying to receive SPARCS Identifiable Data:

Signature:

Printed Name:

Printed Title:

Date Signed:

Contact email address:

When completed, please return signed document to SPARCS.Requests@health.ny.gov

SPARCS Program
Bureau of All Payer Systems and Informatics
Division of Information and Statistics
Office of Quality and Patient Safety
New York State Department of Health
Corning Tower, Rm 1911
Albany, New York 12237