Security Guidelines

The New York State Department of Health (NYSDOH) places a high priority on protecting the data contained within the Statewide Planning and Research Cooperative (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. NYSDOH 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 shall attest annually to continued compliance with 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 Data recipients that fail to maintain compliance or attest may have their permission to SPARCS data rescinded consistent with NYS regulations.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. NYS DOH requires organizations and individuals requesting SPARCS data 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.
3. 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, 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. Logging must comply with NYS Security Logging (NYS-S14-005). 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 Encryption Standard (NYS-S14-007).
6. 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 strong password protection, and be locked after a maximum inactivity period of 15 minutes per NYS Account Management/Access Control (NYS-S14-013).
7. SPARCS data shall not be stored on removable media (i.e., CDs, thumb drives, or other externalstorage 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). Compliance with NYS Bring Your Own Device (BYOD) (NYS-S14-012) is required.

8. Using a cloud hosted or third-party software for geocoding is prohibited unless approved by the Data Governance Committee.
9. Access to approved minimum necessary SPARCS data will be permitted only upon approval of the user's signed individual affidavit. The SPARCS data should be used solely for the purpose(s) stated in the application.
10. SPARCS data shall not be used, accessed, stored, or disclosed unless approved by the Data Governance Committee or SPARCS Program, as applicable. 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 appendix to this affidavit; any request for exception(s) to these Security Guidelines must include information on compensating controls.
11. Upon expiration or recission 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 email to sparcs.requests@health.ny.gov.

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

Date: _____

X _____

Signature of Lead IT Administrator (wet or digital signature required)

Signer's Name (please print) _____

Organization: _____

Email Address: _____

Address: _____

Date _____

X _____

Signature of Organizational Representative (wet or digital signature required)

Signer's Name (please print) _____

Organization: _____

Email Address: _____

Address: _____

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

SPARCS Governance
Bureau of Data Programs and Policy
New York State Department of Health
Corning Tower, Room 1998
Albany, New York 12237

Glossary

Term	Definition
NYS-S14-007 - Encryption Standard	This standard defines requirements for encryption that is used to enhance security and protect the State's electronic data ("data") by transforming readable information ("plaintext") into unintelligible information ("ciphertext").
NYS-S14-013 - Account Management Access Control Standard	This standard establishes the rules and processes for creating, maintaining and controlling the access of a digital identity to NYS applications and resources for means of protecting NYS systems and information.
NYS-S14-005 - Security Logging	This standard defines requirements for security log generation, management, storage, disposal, access, and use. Security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; databases and applications
NYS-S14-012 - Bring Your Own Device	This standard normalizes the management and administration of personal devices accessing state resources.
NYS-S13-003 - Sanitization Secure Disposal Standard	Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.
SPARCS	The Statewide Planning and Research Cooperative System.
SPARCS Data	Three types of SPARCS data available to researchers and others wishing to use the date: 1. Identifiable 2. Limited 3. De-Identified (Public Use)
SPARCS Data Governance Committee	The Data Governance Committee (DGC) is responsible for reviewing SPARCS identifiable data requests. It supersedes the Data Protection Review Board. The DGC is responsible for ensuring the usability, security, and availability of data for all identifiable data requests seeking to use SPARCS data. The Committee follows applicable federal and state laws when determining whether SPARCS data containing identifiable data elements may be shared.
SPARCS program	SPARCS is a comprehensive all payer data reporting system created to collect information on discharges from hospitals. SPARCS currently collects patient level detail on patient characteristics, diagnoses and treatments, services, and charges for each hospital inpatient stay and outpatient (ambulatory surgery, emergency department, and outpatient services) visit; and each ambulatory surgery and outpatient services visit to a hospital extension clinic and diagnostic and

	treatment center licensed to provide ambulatory surgery services.
NYS ITS	New York State Office of Information Technology Services (ITS) was created in 2012 to transform IT services in an effort to make New York State government work smarter for its citizens and enable the state to be accessible for businesses through the use of technology. ITS provides statewide IT strategic direction, directs IT policy and delivers centralized IT products and services that support the mission of the State.