EXHIBIT E

SPARCS SECURITY GUIDELINES

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

This document is provided by DataGen to ensure that organizations with access to SPARCS Data through the Sg2 state data analysis module ("Module") comply with required security protocols. An organizational representative must attest to these data protection standards by initialing next to each provision, and signing the second page of this document.

Completion of this document as written is mandatory, and will attest to your organization's compliance with the following security provisions regarding SPARCS data available in the Module.

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 toor 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 enabledscreensaver 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 DataGen, within a reasonable time, upon request.
	4. All remote connections from offsite locations that access SPARCS data shall be approved in writing by DataGen. 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 SPARCS 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 externalstorage devices), unless approved in writing by DataGen. 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.
	8. Access to the Module 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) of using the Module for the organization.
	9. SPARCS data will not be shared with anyone, in any form, unless approved in advance in writing by DataGen and is in accordance with the SPARCS regulations. The organization's failure to comply with this would constitute a breach in security, and subject the organization to possible penalties.

	10. At the time of termination of the License Agreement, or at such other time as required by notice provided by DataGen, all SPARCS data must be destroyed, 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. Attestation and documentation of the destruction process is required. An extension may be requested via email to DGsupport@hanys.org

Signature of organizational representative authorized to legally bind the organization that is receivingaccess to the SPARCS data through the Module:

Signature:

Printed Name:

Printed Title:

Date Signed:

Contact email address:

When completed, please return signed document to DGsupport@datagen.info

Legal
Division
DataGen,
Inc.
One Empire Drive
Rensselaer, NY 12144