Surgimap

The Physician Driven Imaging Solution

A Nemaris Company

Formal Privacy & Security Assessment

For Surgimap version 2.2.6 and higher

306 East 15th Street Suite 1R, New York, New York 10003

Application Name Surgimap	**Vendor** Nemaris Inc.	**Version** V2.2.6	**Release Date** September 25, 2015

Application supports the following business function(s):

Image viewing and measuring, surgical planning and real time simulated outcomes.

1	Hardware and Software Requirements	
1.1	Can you provide a technical diagram of your system's configuration (Visio preferred)?	We have some PPT presentations that explain the software's configuration
1.2	Is this an ASP (Application Service Provider) model?	No, but we have a licensing server that the software must connect to the first time to activate.
1.3	Does this system run on VMware? What version?	No, Surgimap is supported on its own, using its own cloud server and (Amazon) AWS secure server
1.4	What is the Server OS? Is 64bit OS supported?	Yes, Surgimap will run on a 64bit machine. No server required in-hospital
1.5	Can the system be joined to an existing Active Directory domain? If not does it support LDAP authentication?	No, AD/LDAP authentication is not done. Authentication is done against an online licensing server
1.6	Is there a database component? Which databases are supported? (Oracle, MSSQL Server) What versions are supported?	Surgimap has an internal, encrypted SQLITE database that is managed by the software. No external database is needed.
1.7	Does your system use a web server? What vendor/versions are supported?	No web server is used.
1.8	How many servers are required for this system? What is the function of each server? Does this include a test environment?	There are no minimum required servers for Surgimap. Surgimap downloads directly onto the workstation/computer of an end user's preference.
1.9	What is the expected annual storage growth requirement?	10GB/user/year typically. Storage is local to the user's workstation, and it is encrypted via AES/Blowfish encryption with 256/512 bit keyspace.
1.10	Can the application be installed somewhere other than the C drive?	Surgimap is meant to be installed on the C Drive, but a user also has the option to run Surgimap from a USB stick.
1.11	Does this system run on Citrix? What versions do you support?	The software has been configured to run on Citrix. Although we will provide support to help you configure it, we have not evaluated any specific versions. However, we have multiple customers deployed on Citrix, and it is known to work well with the latest versions.
1.12	Is this application 32 or 64 bit application?	Surgimap is compatible with both 32 and 64 bit environments.

1.13	What Client Operating Systems are supported?	Personal laptops (Windows XP+, Mac OS X 10.7+), iPhone, iPad
1.14	Do files need to be loaded onto individual clients? If so what?	The Surgimap software must be loaded as well as the user database, if not stored locally.
1.15	Is your system compatible with wireless? Does it support 802.11n? Can it support certificate based authentication?	Yes, Surgimap is compatible with wireless machines.
1.16	What files or folders do we need to back up in order for successful recovery? Can you explain your recommended backup strategy?	SurgimapDatabase folder contains all of the user's encrypted files (images + metadata + configuration). Backing up this directory and restoring it into a client version of the software will copy all necessary information in order to restore a working copy of Surgimap.
1.17	Firewall/VPN – does your system require outbound or inbound connectivity? List ports, protocol, and ip addresses	Please see the PACs connection guidelines that can be found at http://surgimapspine.com/support/it-department/. This gives you all the information you need to run Surgimap from behind hospital firewalls.
1.18	Are there any HL7 interfaces for this system?	N/A
1.19	Are there any other interfaces for this system?	N/A
1.20	What is your licensing model? (per seat, concurrent user)	per-user
2	**Printers & Special Hardware**	
2.1	What printers are compatible with this system?	N/A. Surgimap does not have a print feature.
2.2	Are there any special labels required?	No.
2.3	What special hardware is required to use this system, if any? (touch screens, wands, scanners, readers, faxing, etc.)	No special hardware is needed to run Surgimap.
2.4	Special hardware modules to be installed on server? Does it require a separate server? Will it fit in a 1U, 2U server?	No.
2.5	Are any handheld devices used with this system?	Surgimap works on Mac and Windows computers. It is also compatible with the iPhone and iPad, and the app is available on the Apple App store. However, surgeons can only use the desktop version in order to link with their PACS system.
3	**Support**	
3.1	Does vendor need remote access to the system?	No.
3.2	Is this only for initial configuration?	n/a
3.3	What is your support model if any?	Surgimap directly helps its clients with any issues that they are experiencing and it provides WebEx trainings and demonstrations of the software if requested by client.

3.4	Is remote access needed for clients & servers?	No.
3.5	Is a dedicated, point to point connection required to exchange transactions, etc. for this system?	It is only required if the end user would like to connect PACs with Surgimap.
3.6	What is your web site URL?	https://www.surgimap.com
3.7	Do you have a support number?	646-794-8650
3.8	What is our client ID?	n/a
3.9	Who is responsible for supporting this application?(client/vendor) If both who is responsible for the following 1) Hardware 2) Operating System 3) Patching 4) Software/Application Updates 5) Antivirus	Client is respons ble for supporting the Surgimap application. Surgimap pushes out software/application updates every few months. The client will see a notification about an available update when he or she launches the software.
3.10	How many installs of this system exists today?	n/a
4	**Privacy and Health Information Management**	
4.1	Will your system contain patient demographic information?	No
4.2	Will your system be used to document treatment information? If yes, can your system interface with Cerner?	Only if client decides to include this information
4.3	What is the retention period for information stored on your system?	Information is stored on the local computer/drive where it is installed. The information will remain on that local device, unless it is deleted by user.
4.4	If the information is archived, is it easily retrievable?	Information is not archived.
4.5	Will your system contain patient images, readings, voice files, or videos?	Yes.
4.6	Does the client have the ability to modify fields?	Yes.
Questions 4.7 through 4.8 apply to Studies and Surveys *(If this request relates to a study and/or survey, then continue with 4.**7**; If not, continue with 5.1)*		
4.7	What are the fields contained in the survey?	n/a
4.8	Will any patient identifiable information be captured? If yes, will the information be sold to other companies?	n/a
5	**Access Management**	

5.1	Does the application support integration with the enterprise identity management system?	N/A
	a. If yes, indicate the alert (such as Directory Services, LDAP, Kerberos, etc.):	
5.2	Is user authentication controlled by means other than user account and password or PIN?	No
	a. If yes, indicate what other mechanisms are used (e.g. certificates, token, biometric, etc.):	
Questions 5.3 through 5.8 apply to the use of passwords		
5.3	Does the application force “new” users to change their password upon first login into the application?	Before launching the software, the user has to register his or her email and create a password. The user then receives an activation email, after which time the user provides information and agrees to our Terms & Conditions. Only after this is the user able to gain access to the software.
5.4	Can the user change their password at any time?	Yes.
5.5	Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?	Surgimap software has password requirements: 7 letters in length, 1 number, 1 upper case letter.
5.6	Can the application force password expiration and prevent users from reusing a password?	No.
5.7	Is password transmission and storage encrypted and unviewable even to the system administrators?	Yes, passwords are stored as a one-way hashed bcrypt’ed value and transmitted over SSL.
5.8	Can the application be set to automatically lock a user’s account after a predetermined number of consecutive unsuccessful logon attempts?	Yes, after 3 failed log-in attempts, the user is locked out of the account and has to follow specific steps to create a new password to regain access to the account.
5.9	Does the application proh bit users from logging into the application on more than one workstation at the same time with the same user ID?	No.
5.10	Can the application be set to automatically log a user off the application after a predefined period of inactivity?	No, but this is something we are in the process of developing.
5.11	Can access be defined based upon the user’s job role? (Role-based Access Controls (RBAC))?	n/a
	a. If yes, can application generate the list of users by job role?	
5.12	Can the application support the removal of a user’s access privileges without	n/a

	requiring deletion of the user account?	
5.13	Does the application support a mechanism for allowing emergency access by a caregiver to a patient's electronic health information that is not included within their standard access privileges?	No.
	a. If yes, does the application capture and retain details pertaining to this action for review?	
	b. If yes, do the caregiver's access privileges revert back to the original setting upon next log-in?	
6	**Audit Capabilities**	
6.1	Is audit log tracking a feature available in the current version of this software application? *If yes, then continue with **6.2**; If no, continue with **7.0***	No
6.2	Capturing user access activity such as successful logon, logoff, and unsuccessful logon attempts?	See 6.1.
	a. If yes, list the data elements contained in the audit log:	
6.3	Capturing data access inquiry activity such as screens viewed and reports printed?	See 6.1.
	a. If yes, list the data elements contained in the audit log:	
6.4	Capturing data entries, changes, and deletions?	See 6.1.
	a. If yes, list the data elements contained in the audit log:	
6.5	Does the application time stamp for audit log entries synchronize with other applications and systems using NTP/SNTP?	See 6.1.
6.6	Are audit log reports available for the current version of this software application?	See 6.1.
	a. If yes, specify the types of reports.	
	b. If yes, indicate if additional hardware or software (including any third-party software) is required to activate or utilize the audit logging and/or	

	reporting feature.	
6.7	Can the audit log "data" be exported from the application for further processing (e.g. storage, analysis)?	See 6.1.
6.8	Indicate how audit log files are protected from unauthorized alteration:	See 6.1.
6.9	Does the application allow a system administrator to set the inclusion or exclusion of audited events based on organizational policy and operating requirements or limits?	See 6.1.
6.10	Can the application continue normal operation even when security audit capability is non-functional? (For example, if the audit log reaches capacity, the application should continue to operate and should either suspend logging, start a new log or begin overwriting the existing log)	See 6.1.
7	**Security of Remote Access and Support**	
7.1	Which connection method(s) are used to accomplish remote support?	
	a. Dial-up	
	b. Secure web tunneling	
	c. VPN Client (specify VPN technology method here)	
	d. Business-to-business VPN using IPSec	
	e. Other (please explain)	We use WebEx for all support calls.
7.2	Identify which remote support applications are utilized and the security controls enabled:	N/A
7.3	Is functionality built into the application which allows remote user access and/or control?	No
7.4	If requested, can the application associate remote support activities with an individual employee of the vendor? (accountability)	n/a

7.5	Do vendor support personnel have specific roles and accesses that control access to ePHI? *(See section 5.11)*	No, there should be no ePHI data communication. It is worth noting that all Surgimap employees are HIPAA trained before they are ever allowed to access or handle ePHI.
7.6	Does the audit system log remote support connection attempts and remote support actions such as application or configuration modifications?	n/a
8	**Protection from Malicious Code**	
8.1	Is the application compatible with commercial off the shelf (COTS) virus scanning software products for removal and prevention from malicious code?	Yes, Surgimap will run on devices with virus scanning software.
	a. If no, indicate what additional security controls are included with the application/system used to mitigate the risks associated with malicious code:	
8.2	Does the application's client software operate without requiring the user to have local administrator level rights in order to run the application?	Yes, if the software is installed in a location where the local user has write-access. If the application is installed in the Program Files directory, then administrative access is required to write there.
9	**Configuration Management and Change Control**	
9.1	Are updates to application software and/or the operating system controlled by a **mutual** agreement between the support vendor and the application owner?	Yes. When users first create an account with Surgimap they must agree to the terms and conditions of the software. This includes, but is not limited to, updates to the application.
9.2	Has the application been tested to be fully functional residing on its associated operating system/middleware platform configured with a recognized security configuration benchmark?	Surgimap is fully tested and works with Windows XP and newer operating systems. L kewise, it is fully tested and works on Mac OS X 10.7 and newer Mac operating systems.
	a. If yes, indicate the configuration benchmark:	Windows XP+, Mac OS X 10.7+ using internal test suite.
9.3	Can the operating system hosting the application (server or client) be updated by the user without voiding the application warranty or support agreement?	Yes.
	a. If no, will operating system changes, updates, and patches be provided by the vendor?	
9.4	Indicate how updates to the application are typically handled:	If software updates are available, the user will receive a notification to upgrade the software when they launch the program (i.e., before they log-in).

9.5	Indicate how the application is certified to perform as intended with updates to the operating system and other helper applications (such as service packs and hot fixes) and how the customer is notified of this information.	We cryptographically sign and validate our updates per FDA recommendation using RSA 2048 bit signatures of the MD5 hash
10	**Data Export and Transfer Capabilities**	
10.1	Does the application encrypt data before sending it over the Internet or an open network?	Yes.
	a. If yes, indicate the encryption used:	256-bit SSL certificate
10.2	Does the application encrypt data before storing on removable media such as backup tapes, CDs, DVDs, etc. or devices such as laptops, tablets, or computer workstation hard disk drives?	Yes.
	a. If yes, indicate the encryption used:	SQLite Encryption Extension, images using Blowfish.
10.3	Indicate the interfacing and format standards the application can accept or use for transferring data: (e.g., HL7 transaction formats, ANSI X.12 standards, CCOW, etc.):	n/a
10.4	If the application includes a web interface, then identify the type(s) of secure connection supported:	This question is only applicable if you, the user, seek to use Surgimap Access.
11	**Other Capabilities**	
11.1	Does the application maintain a journal of transactions or snapshots of data between backup intervals?	n/a
11.2	Can the system administrator reconfigure to nonstandard port assignments other than the list of registered ports published by IANA?	n/a
11.3	Does the application provide for integration into standard network domain structures?	n/a
11.4	Has the application security controls been tested by a third party?	Surgimap uses internal testing only.
11.5	Does the application have ability to run a backup concurrently with the operation	Yes, the database is synced to disk transactionally, so only complete data is ever found on disk. Backup can

	of the application?	therefore run concurrently
11.6	Does the application include documentation that explains error or messages to users and system administrators and information on what actions required?	Please see the Surgimap user guide in the “IT Department” section of the web site.