Vendor Assessment Questionnaire
Required for all data exchange with third-parties and/or Cloud hosted & SaaS solutions.

Vendor/Partner Name:	Nemaris Inc uses Amazon Web Services for its Surgimap software cloud storage solution	
Solution Description:	Surgimap Access (www.surgimap.com/access)	
Use Case Summary:	Users who have Surgimap installed on their PC can sync their work to collaborators e.g., surgeon to co-surgeons, NP, PA, industry rep using our Amazon cloud solution. When on our cloud the user can also see their work. This allows surgeon to plan their surgery and simulate the patient surgery on their PC, and then when in the OR view their plan by logging into the cloud version	

Data			**Vendor Response**
Data Exchange	1	What types of data will be exchanged between the Surgimap and vendor? (PHI, PCI, Financial, Privacy elements etc.)	The Surgimap software allows Surgeons to measure patient images and apply simulations. If a user wants to sync their work to our cloud solution then any data they enter into Surgimap is encrypted and stored on our AWS server. In practical terms, user will enter the patient name as a means of finding their patient images and that data is encrypted and could be shared to the vendor servers if the user opts to do so. Surgimap does not use patient Soc Sec #, no credit card, no billing info.
	2	How will data be exchanged with the vendor? (secure FTP, web portal, web service etc.)	HTTPS
	3	Approximately how much data or how many records will be stored with the vendor over the course of 1 year?	Only data that the users wants to store on the vendor AWS cloud servers will be uploaded. Most work resides locally with the user. We anticipate that up to 50 patients with up to 4 x-ray images per patient could be synced and stored (but not shared) with vendor over the course of 1 year.

	4	How will the data be used by the vendor? Will it be sent to a third or fourth party?	Data will not be used by the vendor. Data shared to vendor using our Sync feature is only for the purpose of user being able to see their patient images on our cloud solution or for the user to be able to then push that work to their iOS device or share their work with collaborators i.e., co-surgeon, NP, PA. Data sync from user A to user B is via our AWS cloud solution and as such, data is shared to vendor allowing vendor to push into the other user accounts.
Integration/API	5	What API integration or interfaces are required with vendor's servers or systems? (e.g. Web Services, REST, SOAP, DICOM, HL7, custom API etc.)	Available but not required: DICOM
	6	What of vendor's systems will this solution interface or integrate with?	None are required however typically users want to work with DICOM images and as such they will link Surgimap to their PACS solution via a DICOM node
	7	How will API integration or interfaces be secured and authenticated? (e.g. HTTPS, certificate auth, API key or session tokens etc.)	HTTPS and session tokens
Data Protection	8	Will vendor's stored data be encrypted? How? (encryption algorithm, media type, DB encryption used etc.)	Surgimap software uses 256 bit encryption. Surgimap cloud uses HTTPS
	9	What type of encryption is used for transmitted data? (e.g. HTTPS, SFTP)	HTTPS
	#	Are backups encrypted? How long are backups retained?	Yes, all data is encrypted at all times i.e., at rest and when in flight. All data is stored and retained as per HIPAA guidelines.
	##	Will vendor's data or backups be stored outside the United States?	No, we use Amazon AWS in USA
	##	How will vendor's data be segmented/segregated from other vendor customer data?	The majority of data is stored locally by user in their Surgimap account on their PC. Only data that is synced to vendor AWS cloud server is stored online. Data stored online is based on a user account i.e., email address which is the account ID. All user data is stored in same AWS server.

	#	Is data stored or cached with another company or third party? (e.g. Rackspace, Amazon hosting, Akamai CDN etc.)	Yes, all data is stored at Amazon. There is no data stored at Nemaris Inc. The Surgimap data is either stored locally by user on their PC or at Amazon AWS.
	##	What types of data can users or staff download, export or save to computers or mobile devices from the application or solution?	Users who have signed into their Surgimap account can download all of their data i.e., any images, notes, and spine measurements. This can be exported and saved to other computers as images (DICOM, JPEG, BMP,..) or data e.g., excel file.
	##	What types of data can users or staff change or upload to this application or solution?	Users can upload any data they want and modify any of their own data. The user can upload images (DICOM, JPEG, BM,…), videos, text notes and modify their own information. DICOM tags can not be modified since they are attached to the DICOM image as read only.
	##	Will offshore contractors, developers or support staff have access to, process, or store vendor's data or information resources? Data type? Medicare data?	No
	##	Can SSL 3.0 and lower disabled? (TLS 1.1 and higher required, TLS 1.2 preferred)	Surgimap uses TLS 1.2
Vendor Security Polices			**Vendor Response**

Polices & Procedures	1	Please describe information security controls, safeguards and polices in place to safeguard sensitive data including: - Data center access and perimeter controls (including 3rd party hosting such as Rackspace etc.) - User access controls, elevated access account controls (including role management 3rd party hosting such as AWS, Azure if used) - Account monitoring/logging - Secure configuration - network devices & servers - Data protection for vendors laptops, portable media, cloud sync/storage - Malware defenses - Incident response - Secure app development practices - Breach notification procedures to customers	All data is stored on a HIPAA compliant server at Amazon. Amazon has extensive physical and virtual security procedures in place. All cloud access is monitored and tracked i.e., login/logout logs. All data is encrypted 256 bit at rest within Surgimap. AWS has reports of any incidents and will supply breach notifications to customers.
Virtual Sys Management	2	How are virtual cloud based endpoints and networks secured? (e.g. AWS, Azure, Rackspace, Spark environments) (inclusive of cloud based endpoint security agents, unique complex local admin accounts, cloud logging etc.)	Amazon Web Services
	3	How does the vendor maintain admin role and segregation of duties for backend administration of virtual cloud environments? (inclusive of AWS, Azure, Rackspace, Spark roles/groups, unique IDs etc.)	Amazon Web Services
	4	How does the vendor limit access to backend administrative control elements or portals for cloud based virtual environments? (e.g. MPLS to Amazon, VPN, IP restrictions etc.)	Only users have access to their cloud data. In addition vendor admins have access to the AWS servers for server maintenance as well as for customer support duties e.g., to help create an account, turn on premium features, disable / transfer an account

Remote Access ('to' vendor)	5	How is remote access to vendor systems by 3rd parties managed to prevent unauthorized access to the vendor's infrastructure? (e.g. vendor's developers, vendor staff, contractors, HVAC, building maintenance, etc.)	No data resides with vendor. Vendor systems and infrastructure reside on local encrypted, password protected servers.
IDS/IPS	6	How does the vendor utilize IDS/IPS, Firewalls, or similar technical controls in a security best practice/layered approach?	Following AWS protocols
Vuln Mgmt.	7	Explain the vendor's vulnerability management procedures for Internet facing systems & app development practices.	Vendor has policies and procedures in place for its Quality System however since Surgimap cloud solution is only at AWS all Amazon policies and procedures apply
PEN Testing	8	How often does the vendor perform third party penetration (PEN) security testing of Internet facing applications?	AWS conducts ongoing vulnerability testing
	9	Can vendor review the most recent PEN test summary report or independent attestation of validation of PEN testing?	N/A
Data Breach	#	Has the vendor experienced a data breach in the last 24 months or is the vendor a subsidiary of company that has had a breach in the last 24 mths.?	No
Data Sanitization	##	Does the vendor provide published procedures for the return of vendor data, and sanitization of all vendor computing resources of vendor data upon exiting the business relationship?	Surgimap resides locally on vendor and only user requested data (a subset of total data) is stored on AWS. If user deletes data locally it will trigger a delete at AWS of that same record (images, notes, etc). There is nothing to return once user has deleted their data.
	##	How is customer data secured when responding to requests from law enforcement or other third parties? (e.g. Attorney etc.)	Surgimap will comply with all official law enforcement requests in accordance to HIPAA rules
Regulatory	##	Will the Surgimap allow vendor to view SSAE 16, SOC 1, SOC 2 or similar third party compliance assertion/attestation summaries?	Yes, when available

	#	Has the vendor/organization been under an OIG investigation or a corporate integrity agreement (CIA) in the last 5 years?	No
Contracts	##	Does a business contract exist or is one in progress for this Surgimap with Vendor's Legal/Contract Management?	Surgimap is freeware. No business contract exists however we can sign a separate BAA if required
	##	Is Surgimap willing to sign the vendor's BAA (HIPAA Business Associate Agreement) ?	Yes
Usage & Authentication		***** this section may not apply if data exchange only with vendor and web based portals/logins are not part of this solution*****	**Vendor Response**
Use Case	2	Will vendor's staff have user or administrative access to this application/solution? If yes - How will staff authenticate?	Any user can create their own account and have access to this freeware. Users simply need to register and can then access their own data via a User ID and password. If user shares their credentials with vendor's staff or their administrative team, then they too will have access to the user data.
SSO	3	Will SSO via PING Federate, SAML 2.0 be used for identity integration and authentication?	N/A
	4	For SAML/PING SSO; a) Is Kerberos auth supported for the PING connector authentication vendor's side? b) How many customers have you setup with SAML 2.0? c) What type of Service Provider do you use? d) What type of attributes do you expect in the assertion? e) Do you support Deep Linking with Service Provider Redirection? f) Explain initial user load and user account add/remove process options	N/A

	5	If SSO not used - explain options for password complexity, rotation/expiration, lockout, password reset and web session timeout settings.	Currently Surgimap uses 8 char or longer password with minimum of 1 upper case, 1 lower case, and 1 number. Rules can be implemented requiring rotation / expiration. Password reset is done by user clicking link on login page which will send a reset email to email address on file. Web session timeout is less than 2 min of inactivity.
Account Admin	6	How will users be provisioned, de-provisioned and how are access roles assigned or granted? Active Directory Group role mapping possible? (initial user load and user account add/remove)	Users create their own accounts by visiting www.surgimap.com/access and following the onscreen registration process. Group creation of accounts can be done by vendor
	7	How does the vendor store login ID's and passwords? (e.g. Oracle, SQL, Active Directory, encrypted? hashed?)	AWS, salted and hashed
	8	Explain potential options or support for multifactor authentication such as OTP (One Time Password).	NA for password, only for password reset link
	9	Will users or staff access the hosted solution from outside the vendor's network or from non-vendor's computers or mobile devices? (e.g. personal devices from the Internet)	Potentially. Users can log into their AWS cloud version of Surgimap to view or plan their upcoming cases regardless of where they are.
	#	Explain options to restrict login/access to vendor's corporate devices only.	Surgimap will run on local vendor's computers. Only user selected data will sync to cloud. If vendor does not want users to sync or log into cloud version then it can be mandated to their users. This is same as telling users not to send emails with patient images or names. It needs to be part of vendor's regulatory compliance by all users