Vendor Solution Information Technology Security Questionnaire

Company Information

Company	Nemaris, Inc.		Product	Surgimap
Primary Contact				
Name	Stephen Schwab		Email Address	sschwab@surgimap.com
Office Phone	(646) 794-8648		Cell Phone	(415) 235-5097
Technical Contact				
Name	Raul Macule		Email Address	rmacule@surgimap.com
Office Phone	(646) 794-8650		Cell Phone	
Information Security Contact				
Name	Stephen Schwab		Email Address	sschwab@surgimap.com
Office Phone	(646) 794-8648		Cell Phone	415-235-5097

About This Questionnaire

This Information Security Questionnaire assist the Information Security Officer capture and analyze relevant information about your organization's ability to provide secure solutions and your information security program. The responses also assist the hospital in fulfilling our legal obligations as a regulated entity. In addition to the certification provided below, you will be required to warrant the completeness and accuracy of your answers in any agreement entered into between your company and the hospital.

The hospital acknowledges that the information contained in this document is confidential and may not be disclosed to a third party without permission.

How to Complete This Questionnaire

- Please begin by completely filling in the company information section above.
- Please complete all questions by entering the most accurate answer, providing a complete answer to any question(s) or requests for information, or, as appropriate, both.
- If one part of a question addressing multiple requirements causes you to be unable to answer "Yes," provide such explanatory information as you deem appropriate as a separate file attachment, clearly indicating the question number and part of the question to which it relates.
- If there are any questions you are unclear about, please reach out to your contact on the Hospital Information Security team.
- If there are any questions for which you would like to provide supporting material or additional information, please include a separate attachment, clearly indicating the question number to which it relates.
- Once completed, this document may be returned your Information Security Contact as a file attachment.

1. Technology Solution

#	Information Requested	Information Provided by Vendor
1-1	Main contact from the hospital	N/A
1-2	Description of solution (What business challenge does it solve? How does it work?)	Surgimap is the leading preoperative planning platform for spine. The software allows Surgeons and Researchers to measure patient images and apply simulations for surgical procedures. Surgimap is complementary with PACS and can be directly connected to a PACS through the DICOM Node interface for image import/export (send/query).
1-3	Departments using the solution	Spine
1-4	What infrastructure changes, if any, will this solution require? Examples of infrastructure changes include VPN's, Firewall Rules, etc. Please include specifics such as transmission protocols, service accounts on our domain and appliances.	Allow access to these domains: 1. https://www.surgimap.com/api 2. http://www.surgimap.com/api And to these ports: 1. api.surgimap.com TCP port 8080 SSL 2. www.surgimap.com TCP port 80 HTTP 3. www.surgimap.com TCP port 443 SSL 4. surgimapaccess.s3.amazonaws.com TCP port 80 HTTP 5. surgimapaccess.s3.amazonaws.com TCP port 443 SSL
1-5	What changes will be required to our desktop configurations such as local administrator access or group policy changes.	Surgimap can be installed locally. Please allow read & write permission to the location where Surgimap is saved.
1-6	Will this solution require that your implementation or support require permanent access to our network and/or network resources? If so, please describe what access will be needed, by whom, and for what purposes. Please also describe how access for these individuals will be requested, changed and removed when they no longer need access.	No
1-7	Will this solution require the creation of any accounts used by more than one person?	No, each user creates their own Surgimap account associated to their email address.
1-8	Is there any reason why any equipment required to be added to our network will not be able to run our Anti-Virus Software (currently Symantec Endpoint Protection) and communicate with our antivirus management system.	No
1-9	Our organization uses Symantec Endpoint Protection (SEP) on all hosts. What issues does this	None

	solution have that would prevent enablement of any SEP components?	
1-10	What web browsers (if required) are tested and supported.	N/A

2. Data Requirements

Vendors often outsource or partner with other firms to provide services or products. Some examples include server co-location providers, hosting companies, application service providers, etc.

Provide the following information about the data transmitted, accessed, or stored by your solution.

List all business partners that store/transmit data in the last column

#	Data Type	Transmits or Accesses (Y/N)	Stores Offsite (Y/N and if yes, provide Data Center Location(s) and owner)	Accessed or stored by business partner (Provide business partner name)
2-1	Protected Health Information (PHI)	Y	N	N
2-2	Personally Identifiable Information (PII)	Y	N	N
2-3	Social Security Numbers (SSN)	N	N	N
2-4	Payment Card Information	N	N	N
2-5	Confidential Technology Information	N	N	N
2-6	Hospital Mission Critical Information	N	N	N
2-7	Business Critical Information	N	N	N
2-8	Other Sensitive Information	N	N	N
2-9	Public Information	N	N	N

3. Independent Security Certifications

Please provide the following information about the independent security certifications of your organization and each business partner and data center listed in Section 2. Examples of independent evaluations include, but are not limited to HITRUST, SSAE 16, ISO 2700x, etc. Add lines if needed

#	Company	Certification	Audit Firm	Date
3-1	Nemaris Inc.	ISO Certificate Q5 18 04 76406 006	ISO	6/22/2018
3-2	Nemaris Inc.	EC Certificate G1 18 04 76406 007	EC	6/22/2018
3-3	Nemaris Inc.	EG Zertifikat G1 18 04 76406 007	EG	6/22/2018
3-4	Nemaris Inc.	ISO Zertifikat Q5 18 04 76406 006	ISO	6/22/2018
3-5				
3-6				
3-7				
3-8				
3-9				

If all of the companies listed above have independent certification of their internal security controls, Completion of section 4 may not be necessary.

4. Security Controls for hosted solution

Please provide the following information and comments (optional) about the security controls. **Important: This section must be filled out separately for each organization, listed in Section 3, unless they have been certified by an accredited agency**, such as:

- HITRUST
- SSAE 16
- ISO 2700x
- CSI
- or other agency approved by the hospital's Information Security Officer

****Please include independent security certification documentation in response if the questions are not completed****

If this solution does not have a hosted/cloud based component, you may skip to section 5.

#	Controls	Y/N/NA	Comments
	Company Information		
4-1	Will accommodate an onsite visit for a security audit within 24 hours' notice.	N/A	Surgimap is running locally on hospital computers with no cloud sync, therefore section 4 is not applicable.
4-2	Will store all hospital confidential data within US - incl. backups.		
4-3	Maintains an audit log for the location of all confidential data and their backups, to identify where it is located at any point in time, in order to address privacy laws for storage within United States		
4-4	Will not access hospital confidential data from outside of United States.		
	Policies, Standards and Procedures. The vendor:		
4-5	Has formal written Information Security Policies.		
4-6	Has an established process to receive and address vulnerabilities from external organizations?		
4-7	Has an established process to disclose vendor or externally identified vulnerabilities to the hospital?		
4-8	Are identified vulnerabilities required to have a documented remediation plan?		
4-9	Maintains incident response procedures.		
4-10	Has a policy to protect client information against unauthorized access; whether stored, printed, spoken or transmitted.		
4-11	Has a policy that prohibits sharing of individual accounts and passwords.		

4-12	Has a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances.		
4-13	Performs background checks for individuals handling confidential information.		
4-14	Has termination or job transfer procedures that immediately protect unauthorized access to information.		
4-15	Provides customer support with escalation procedures.		
4-16	Has documented change control processes.		
4-17	Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements.		
4-18	Has a policy that implements federal and state regulatory requirements.		
4-19	Maintains a routine user Information Security awareness program.		
4-20	Has a formal routine Information Security risk management program for risk assessments and risk management.		
	Architecture. The vendor:		
4-21	Will provide a network topology diagram/design for any location where hospital data will travel.		
4-22	Implements network firewall protection on all networks that contain hospital data.		
4-23	Implements web application firewall protection for applications that store hospital data.		
4-24	Provides network redundancy for vendor hosted hospital information that is transmitted to end users to fulfill their job functions.		
4-25	Has IDS/IPS technology implemented for networks that store confidential hospital information.		
4-26	Uses DMZ architecture for Internet systems for networks that store confidential hospital information.		
4-27	Adheres to the practice that web applications, which 'face' the Internet, are on a server different from the one that contains the database with hospital information.		

4-28	Uses enterprise virus protection on all systems.		
4-29	Follows a program of enterprise patch management.		
4-30	Provides dedicated customer servers to segregate data from other customer data. If not then how is this accomplished in a secure virtual or segmented configuration.		
4-31	Implements controls to restrict access to data from other customers.		
4-32	Ensures that remote access is only possible over secure connections.		
4-33	Has managed, secure access points on its wireless network that contains hospital data.		
	Configurations for Hospital Facing Devices The vendor:		
4-34	Implements encryption processes for data in motion, which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others, which are Federal Information Processing Standards (FIPS) 140-2, validated.		
4-35	Implements encryption for confidential information at rest that satisfy *NIST Special Publication 800-111*.		
4-36	Has password-protected screen savers that activate automatically to prevent unauthorized access when idle, for computers used by system's support users.		
4-37	Removes all unnecessary services from computers.		
4-38	Uses file integrity monitoring software on servers (such as tripwire, etc.) for any hospital data subject to PCI standards.		
4-39	Changes or disables all vendor-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products.		
4-40	Uses passwords that are a min of 8 characters, expires at least annually & have complexity requirements: a. 8 Characters or greater b. At least one numeric, one alphanumeric and one special character c. One upper and one lower case value		

4-41	Ensures that passwords are never stored in clear text or are easily decipherable.		
4-42	Do you enforce an easily guessable password filter?		
4-43	Checks all systems and software to determine whether appropriate security settings are enabled.		
4-44	Manages file and directory permissions following least privilege and need-to-know practices.		
4-45	Implements redundancy or high availability for critical functions.		
4-46	Authenticates all user access with either a password, token or biometrics.		
4-47	Formally approves tests and logs all system changes.		
4-48	Does not use production data for both development and testing, unless the customer has approved it.		
4-49	Uses artificial data in both development and test environments.		
4-50	Secures development and test environments using, at a minimum, equivalent security controls as the production environment.		
4-51	Uses separate physical and logical development, test and production environments and databases.		
4-52	Limits access to development and test environments to personnel with a need to know.		
4-53	Sets the account lockout feature for successive failed logon attempts on all system's support computers.		
4-54	Prohibits split tunneling when connecting to customer networks.		
	Product Design. The vendor:		
4-55	Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access. The encryption technology satisfies *NIST Special Publication 800-111*.		
4-56	Ensures that access to confidential information, across a public connection, is encrypted with a secured connection and requires user authentication. The encryption technology complies, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-		

	77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.		
4-57	Implements protections for Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.		
4-58	Audits the application against the OWASP Top 10 Application Security Risks.		
4-59	Ensures that application server and database software technologies are kept up-to-date with the latest security patches.		
4-60	Uses threat modeling in their software development lifecycle (SDLC).		
4-61	Performs security code reviews as part of their SDLC.		
4-62	Conducts OWASP code reviews for the Top 9 source code flaw categories as part of their SDLC.		
4-63	Does your application follow a coding standard? If so, what standard does it follow?		
4-64	Does the API require an API key per request?		
4-65	Do API requests go through input validation?		
4-66	Do API requests or responses go through content type validation?		
	Compliance. The vendor:		
4-67	Can provide 3rd party documentation that its product is HIPAA compliant, if the vendor manages any PHI on behalf of the hospital.		
4-68	Can provide documentation of its PCI-DSS compliance if the vendor manages any payment card information, on behalf of the hospital.		
	Access Control to the hospital's network or data. The vendor:		
4-69	Contacts hospital or removes, or modifies access, when personnel terminate, transfer, or change job functions within 24 hours.		
4-71	Achieves individual accountability by assigning unique IDs and prohibiting password sharing.		
4-72	Ensures that critical data, or systems, are accessible by at least two trusted and authorized individuals, in order to limit having a single point of service failure.		

4-73	Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.		
4-74	Ensures that all administrative tasks, completed with privileged access, are logged and made available for troubleshooting.		
	Monitoring servers on networks connect to hospital or devices that store or transmit hospital data. The vendor:		
4-75	Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.		
4-76	Reviews system logs for failed logins, or failed access attempts monthly.		
4-77	Reviews and removes dormant accounts on systems at least monthly.		
4-78	Reviews web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise.		
4-79	Performs scanning for rogue access points at least quarterly.		
	Physical Security of locations with devices connected to the hospital network or storing hospital data. The vendor:		
4-80	Controls access to secure areas. E.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.		
4-82	Controls access to server rooms and follows least privilege and need-to-know practices for those facilities.		
4-83	Has special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.		
4-84	Shreds or incinerates printed confidential information.		
4-85	Prohibits or encrypts confidential information on laptops & mobile devices.		
4-86	Positions desktops, which display confidential information, in order to protect from unauthorized viewing.		
4-87	Escorts all visitors in computer rooms or server areas.		
4-88	Implements appropriate environmental controls, where possible, to manage equipment risks, e.g., fire safety, temperature, humidity, battery backup, etc.		

4-89	Has no external signage indicating the content or value of the server room or any room containing confidential customer information.		
4-90	Provides an export copy of all of the customer's data in a mutually agreed upon format at the end of the contract.		
4-91	Follows forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term.		
	Contingency planning for offsite locations with systems or data used by the hospital. The vendor:		
4-92	Has a written contingency plan for mission critical computing operations.		
4-93	Reviews and updates the contingency plan at least annually.		
4-94	Has written backup procedures and processes.		
4-95	Tests the integrity of backup media quarterly.		
4-96	Stores backup media in a secure manner and controls access.		
4-97	Maintains a documented and tested disaster recovery plan.		
4-98	Uses off-site storage and has documented retrieval procedures for backups.		
4-99	Password protects and encrypts all backups.		
4-100	Provides rapid access to backup data.		
4-101	Labels backup media appropriately, to avoid errors or data exposure.		

5. Security Controls for On Premises Solution

Please provide the following information and comments (optional) about the security controls. **Important: This section must be filled out separately for each organization, listed in Section 3, unless they have been certified by an accredited agency**, such as:

- HITRUST
- SSAE 16
- ISO 2700x
- CSI

- or other agency approved by the hospital's Information Security Officer

#	Controls	Y/N/NA	Comments
	Company Information		
5-1	Will accommodate an onsite visit for a security audit within 24 hours' notice.	N/A	Surgimap is installed on hospital computers. As such, we rely on hospital physical safeguards that unauthorized users do not have access to the surgeon computers. In addition, since SM is running on hospital computers we rely on The Hospital IT dept protocols to protect their network against virus, hacking, and other cybersecurity.
5-2	Does your company have any independent security evaluations? (if so, please provide the most recent independent security evaluation in the comments section)	Y	https://www.surgimap.com/wp-content/uploads/2017/03/Angular-Staging-Remediation-Scan-Report.pdf
5-3	Will this solution require that your implementation or support require permanent access to our network and/or network resources? If so, please describe what access will be needed, by whom, and for what purposes. Please also describe how access for these individuals will be requested, changed and removed when they no longer need access	N	
	Patching.		
5-4	Can you confirm that all operating systems and software are supported by the manufacturer and able to receive all patches and updates? (Provide latest supported Operating System, Database Engine, Other software, such as Java, Tomcat, etc. in the comments)	Y	Windows: Microsoft Windows 7 or newer Mac: Apple Mac OS X 10.10 or newer
5-5	Can critical and routine OS and system security patches be applied as they become available without prior vendor approval?	Y	
5-6	Can security patches or other software be installed remotely?	Y	
5-7	Does your company have a process in place to ensure that upgrades to operating systems and software occur before end of support?	N/A	
	Passwords.		
5-8	Do your systems require that all passwords associated with the solution must meet the hospital's password complexity requirements? a. 8 Characters or greater b. At least one numeric, one alphanumeric and one special character c. One upper and one lower case value	N	Surgimap meets all password complexity requirements except no special characters are permitted. Please note that Surgimap login is in addition to login for individual workstations at the hospital.
5-9	Are password hashes or values protected from non-privileged users?	Y	
5-10	Are passwords stored in encrypted format?	Y	
5-11	Are application passwords encrypted in the database table?	Y	
5-12	Can passwords be viewed in clear text on the screen as the individual types the user ID and password?	N	Passwords are encrypted at all times including during typing.

5-13	Are there hardcoded passwords?	N	
	User Authentication/Authorization.		
5-14	Does the solution require an account logged on at all times for services to function correctly?	Y	
5-15	Does the solution require users to authenticate to gain access to the application/system?	Y	
5-16	Does the solution have the ability to assign a unique username and password authenticated by the hospital's Active Directory? For non-Active Directory compliant devices a unique username and password is still required.	N	A unique username and password is required for Surgimap login although this is not authenticated by the hospital's Active Directory.
5-17	Does application support use of Secure LDAP?	N/A	
5-18	Can you confirm this solution does not require the use of well-known privileged accounts (root, sa, oracle, etc.) - equivalent access level is acceptable?	Y	Does not require the use of well-known privileged accounts
5-19	Can you confirm that no generic accounts are required by the solution?	Y	
5-20	Will this solution require the creation of any accounts used by more than one person?	N	
5-21	Are there different levels of access or user roles defined in the application?	Y	
5-22	Are special privileges assigned directly within the system to control what users are able to see and do?	N	
5-23	Is an administrator or power user account required to operate the device?	N	
5-24	Are authentication attempts performed over a secure channel (no clear text communications of credentials)?	Y	
5-25	Can the solution alert the system administrator regarding any unauthorized access to medical records?	N/A	
5-26	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Y	Surgimap is secondary to hospital computer log out after predetermined length of inactivity. Only a user that is logged into a hospital computer can log into Surgimap. In addition to hospital logout for inactivity, Surgimap also will log the user out after 30 minutes of inactivity.
5-27	Does the solution require service accounts (application, database, operating system)?	N	
5-28	Are service accounts denied interactive mode?	N/A	

5-29	Achieves individual accountability by assigning unique IDs and prohibiting password sharing	Y	
	Administrator rights.		
5-30	Can the device owner/operator (administrator) reconfigure product security capabilities?	No	
5-31	Can we create a specific OS user with administrator rights to allow access for monitoring, configuration and recovery purposes?	No	
	Audit Logging		
5-32	Does this solution provide audit logging capabilities? If so what logging capabilities (ex. Administrator activities)	No	
5-33	How long are logs retained?	N/A	
5-34	Can audit trail logs be archived or stored off-line and recalled as needed?	N/A	
5-35	Are audit logs protected from manipulation?	N/A	
5-36	Does the solution log events such as accessing, reading, and writing patient information?	N/A	
5-37	Is login/logout recorded in audit log?	N/A	For those who authenticate themselves against our Amazon AWS, we do capture login attempts.
5-38	Is every unsuccessful login attempt recorded in audit log?	N/A	For those who authenticate themselves against our Amazon AWS, we do capture login attempts.
5-39	Is remote service activity recorded in audit log?	No	
5-40	Does the solution maintain an audit trail of all security maintenance performed by date, time, user ID, device and location and information is easily accessible?	No	
5-41	Does this solution support exporting of logs to 3rd party logging tools? (If so what format)	No	
	Hardening.		
5-42	Does the solution employ any hardening measures? Please, indicate in the notes the level of conformance to any industry-recognized hardening standards.	No	
5-43	Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?	N/A	
5-44	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet	N/A	

	Explorer, etc.) which are not required for the intended use of the device deleted/disabled?		
5-45	Are all communication ports which are not required for the intended use of the device closed/disabled?	N/A	
5-46	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	N/A	
5-47	Are all shared resources (e.g., file shares) which are not required for the intended use of the device, disabled?	N/A	
5-48	Does the solution have external communication capability (e.g., network, modem, etc.)?	N/A	
5-49	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	N/A	
5-50	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	N/A	
5-51	Does the device employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	N/A	
5-52	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	N/A	
5-53	Can the hospital install host-based security components such as a firewall, host intrusion prevention system (HIPS), anti-malware software, and/or any other security suite software required to operate on the our production network?	N/A	
5-54	Can we configure Windows firewall or IPSec filtering for added protection?	N/A	
5-55	Audits the application against the OWASP Top 10 Application Security Risks.	N/A	
5-56	Uses threat modeling in their software development lifecycle (SDLC).	N/A	
5-57	Performs security code reviews as part of their SDLC.	N/A	
5-58	Conducts OWASP code reviews for the Top 9 source code flaw categories as part of their SDLC.	N/A	
5-59	Implements protections for Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.	N/A	

5-60	Does your application follow a coding standard? If so, what standard does it follow?	N/A	
5-61	Does the API require an API key per request?	N/A	
5-62	Do API requests go through input validation?	N/A	
5-63	Do API requests or responses go through content type validation?	N/A	
	Encryption.		
5-64	Can the database be encrypted?	Y	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode.
5-65	Implements encryption processes for data in motion which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.	Y	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode.
5-66	Implements encryption for confidential information at rest that satisfy *NIST Special Publication 800-111*.	Y	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode.
5-67	Is private data encrypted prior to transmission via a network or removable media? (If yes, indicate in the notes which encryption standard is implemented.)	Y	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode.
5-68	Can the hard drive be encrypted?	Y	Surgimap software is a class II medical device and as such encrypts all data using 256-bit encryption at rest as well as in flight. We protect against brute force logins by locking the user's account after 3 failed attempts when in offline mode.
5-69	Do you support 3rd party encryption tools?	N/A	
5-70	Can you confirm all devices requiring a wireless connection must support WPA2 Enterprise encryption and all current radio frequencies?	Y	
5-71	Are hardcoded encryption keys used?	N/A	
	Compliance.		
5-72	Can provide 3rd party documentation that its product is HIPAA compliant, if the vendor manages any PHI on behalf of the hospital.	Y	https://www.surgimap.com/wp-content/uploads/2018/10/AWS_HIPAA_Compliance_Whitepaper.pdf
5-73	Can provide documentation of its PCI-DSS compliance if the vendor manages any payment card information, on behalf of the hospital.	N/A	No payment card information is managed in Surgimap.
	Contingency planning		
5-74	Tests the integrity of backup media quarterly.	Y	

5-75	Stores backup media in a secure manner and controls access.	Y	
5-76	Password protects and encrypts all backups.	Y	
5-77	Provides rapid access to backup data.	Y	
5-78	Labels backup media appropriately, to avoid errors or data exposure.	Y	
	Other.		
5-79	Does the solution incorporate an emergency access ("break glass") feature?	N/A	
5-80	Are instructions available for device/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	N/A	
5-81	How does the proposed system/device ensure integrity?	N/A	
5-82	Product has the ability to enable redundancy or high availability for critical functions?	N/A	
5-83	Do any files need to be excluded from AV real-time scanning?	N/A	
5-84	Uses file integrity monitoring software on servers (such as tripwire, etc.) for any hospital data subject to PCI standards.	N/A	
5-85	Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access. The encryption technology satisfies *NIST Special Publication 800-111*.	N/A	
5-85	Does the solution have wireless capability? If so, what are the available encryption types?	N/A	
5-86	Has an established process to receive and address vulnerabilities from external organizations?	Y	Surgimap has such a process as part of our ISO 13485:2016.
5-87	Has an established process to disclose vendor or externally identified vulnerabilities to the hospital?	Y	Surgimap has such a process as part of our ISO 13485:2016.
5-88	Are identified vulnerabilities required to have a documented remediation plan?	Y	Surgimap has such a process as part of our ISO 13485:2016.

6. Privacy Questions

Please provide the following information and comments (optional) about the privacy information

#	Controls	Y/N/NA	Comments
6-1	Will the system store, transmit, process, or manage information about hospital patients?	Y	Surgeons who use the Surgimap software can store the patient image & name
6-2	Will the hospital be sending you identifiable patient information?	N	All Surgimap data entered by users is stored locally on the hospital workstation
6-3	Does your solution involve any devices that collect information?	Y	Surgimap collects (saves) patient images and ID associated to the image e.g, name or research tracking ID
6-4	Will the hospital's information be segregated from other customer's information when backed up?	Y	The hospital will perform their own computer back-up and store the Surgimap local data in that backup
6-5	Will you sign the hospital's Business Associates Agreement?	Y	Please send it to sschwab@surgimap.com for signature
6-6	Does the system create audit logs (log each event where a user accesses patient information, login, logout, password attempts)?	N	Surgimap is run locally on hospital computers that have their own audit logs
6-7	How are audit logs made available to the hospital's Privacy and Information Security Officer?	N/A	
6-8	Can audit logs be exported to CSV or XML?	N/A	
6-9	How are end user accounts managed, by vendor or by client?	Y	Client (user) creates their own account. The hospital can inform Surgimap when a user has been terminated so that Surgimap can shut down that account. Also, the hospital can delete the local Surgimap to delete any content.
6-10	Since we are a multi-facility site, does your application allow restricting one site from seeing another site's data, if applicable?	Y	Surgimap user data is only locally on the machine where Surgimap is installed and only available to user who has the username and password
6-11	Describe any reporting capability. Can users be restricted from running a report or extract of all information or large number of patients?	Y	Since Surgimap is run locally at the hospital computer, login/access reporting is done by hospital. The Surgimap export feature is disabled for all users and can only be activated upon request.
6-12	Do you log which records are included in a report or extract?	N/A	We do not report on locally activity
6-13	Do you have last logon reports?	Y	Surgimap can track login stats if the port is open.
6-14	Who is notified when our information was at risk of or has been accessed by an unauthorized person?	N/A	Surgeons load their own data into Surgimap on a hospital computer. Existing hospital computer security will prevent unauthorized use. Surgimap also has a

			brute force locking mechanism which is triggered after 5 wrong login attempts.
6-15	Do you provide a report to your customers to demonstrate the evaluation requirement after significant changes or upgrades that potentially affect the security of the system?	Y	Surgimap pushes 4 – 6 updates per year with detailed release notes. Our team is always available to answer specific questions. Our 3rd party security reports are posted on our corporate site within Support –> IT Department
6-16	Does your system automatically log users off after a set amount of time?	Y	
6-17	Is the data you store, process, or transmit used in any other way (identified or de-identified) than in the services described in our RFP or contract?	N/A	Surgimap data is stored locally within the hospital. We do not have access to hospital data.
6-18	Does your services for the hospital include or are related to fundraising or marketing?	N	

I have reviewed our responses to this questionnaire and certify that all information given above is true and complete to the best of my knowledge. I further declare that all due diligence has been exercised in the preparation, gathering, and reporting of the foregoing information. I understand and acknowledge that the hospital will rely on the responses provided above in potentially entering into a relationship with my organization. I represent and warrant that I am authorized by my organization to execute this questionnaire on its behalf.

Typed Name	Title	Email Address
Stephen Schwab	President	sschwab@surgimap.com