THIRD-PARTY ASSESSMENT QUESTIONNAIRE

Dec 2015

NOTE: Prior to finalizing business agreements involving confidential data, this completed form should be submitted with [Vendor's technical response to Company's Information Security Office]

Third-Party Provider Name: Nemaris, Inc. Date: 12/23/2015
Address: 306 E 15th Street #1R New York, NY 10003 Website:www.surgimap.com
IT Security Contact: Anthony Nicholas Malczanek Email: amalczanek @ surgimap_._com Phone: +1 646 794 8650 x206
Location of Data Center: Amazon AWS Virginia US1a Contact:__________________________Phone: __________________
Location of Recovery Center: Amazon AWS Virginia US1a Contact:__________________________Phone: __________________
Company Sponsoring Business Unit ___________________________Contact:___________________________Phone:__________________

Description of Service/Product: Medical image measurement and surgical simulation software.

Users of the System: Surgeons, radiologists, medical implant manufacturer representatives, medical office staff.

Technical Description (client, agent, SSL, FTP transmission, hosted website, ASP, etc.):

Desktop software with connection to Amazon AWS web service

*Describe Pertinent Outsourced/Contracted Service Arrangements: (such as: onsite support, remote support, temporary access, database management, etc.)*____

DATA REQUIREMENTS
(mark a "1" in all boxes applicable for this relationship)

Transmit or Access	**Stores Offsite**	***Risk***	***Data Type***
		High	Protected Health Information (PHI)
		High	Personally Identifiable Information (PII) for Individuals
		High	Social Security Numbers (SSN)
		High	Payment Card Information
		High	Sensitive Digital Research Data
		High	Physical Plant Detail
		High	Institutional Mission Critical Information
		Medium	Business Critical Information
		Medium	Intellectual Property
		Medium	Other Sensitive Information
1	1	Low	Public Information

Answer: 0 = Not Applicable, based on service provided

1 = Yes

2 = Partially

3 = No

Comments: are optional, but may be used to explain answers.

Answer	**Comments**	A. Company Information. The vendor:
0	We are not going to receive nor store any Company confidential data	1. Will store all Company confidential data within US - incl. backups.
0	We are not going to receive nor store any Company confidential data	2. Maintains an audit log for the location of all Company 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
0	We are not going to receive nor store any Company confidential data	3. Will not access Company confidential data from outside of United States.
0		***Total Company Controls***

Answer	**Comments**	B. Policies, Standards and Procedures. The vendor:
1		1. Has formal written Information Security Policies.
1		2. Will provide copies of the Information Security Policies.
2		3. Can provide results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70, pen. test, vulnerability assess., etc.).
1		4. Maintains incident response procedures.
1		5. Has a policy to protect client information against unauthorized access; whether stored, printed, spoken or transmitted.
1		6. Has a policy that prohibits sharing of individual accounts and passwords.
1		7. Has a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances.
1		8. Requires system administrators to be educated and qualified.
1		9. Implements AAA (Authentication, Authorization, Accounting) for all users.
1		10. Performs background checks for individuals handling confidential information.
1		11. Has termination or job transfer procedures that immediately protect unauthorized access to information.
1		12. Provides customer support with escalation procedures.
1		13. Has documented change control processes.

1		14. Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements.
1		15. Has a policy that implements federal and state regulatory requirements.
1		16. Maintains a routine user Information Security awareness program.
1		17. Has a formal routine Information Security risk management program for risk assessments and risk management.
18		***Total Policy Controls***
Answer	**Comments**	C. Architecture. The vendor:
1		1. Will provide a network topology diagram/design.
1	Amazon in DC, SonicWall firewall in office.	2. Implements network firewall protection.
1	Via Amazon	3. Implements web application firewall protection.
1	Via Amazon	4. Implements host firewall protection.
1		5. Maintains routers and ACLs.
1	Via Amazon	6. Provides network redundancy.
0	Software used in hospitals where IDS systems are already in place.	7. Has IDS/IPS technology implemented.
0	We're hosted at Amazon.	8. Uses DMZ architecture for Internet systems.
1	RDS instance is internal to Amazon, DB not hosted on web server.	9. Adheres to the practice that web applications, which 'face' the Internet, are on a server different from the one that contains the database.
0	Software is deployed in hospitals/corporate which include their own enterprise anti-virus protection.	10. Uses enterprise virus protection on all systems.
1		11. Follows a program of enterprise patch management.
2	Data is stored locally, and only data which Company chooses to share with others is added to a database shared between users.	12. Provides dedicated customer servers to segregate Company data from other customer data. If not then how is this accomplished in a secure virtual or segmented configuration.
1		13. Implements controls to restrict access to Company data from other customers.
1	SSL, SSH, VPN	14. Ensures that remote access is only possible over secure connections.
1	Local test / dev, Amazon production.	15. Uses separate physical and logical development, test and production environments and databases.

1	Same configuration as live, except on different servers.	16. Secures development and test environments using, at a minimum, equivalent security controls as the production environment.
1		17. Will provide the architectural software solution design with security controls.
1		18. Has managed, secure access points on its wireless network.
16		***Total Architecture Controls***
Answer	**Comments**	D. Configurations. The vendor:
1		1. Implements encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit or uses TLS 1.0, preferably TLS 1.1.
1	We use SQLite Encryption Extension with 128-bit encryption for our 2015 release, 256bit AES for our 2016 release for local data encryption, and 512-bit Blowfish encryption for image encryption	2. Implements encryption for confidential information at rest with a strength of at least AES 256 bit.
1	Software is run on hospital computers that automatically log out after a certain amount of inactivity	3. Has password-protected screen savers that activate automatically to prevent unauthorized access when idle, for computers used by system's support users.
1		4. Removes all unnecessary services from servers.
3	We monitor existing logs from web server and API for intrusion detection. Can be implemented for a fee.	5. Uses file integrity monitoring software on servers (such as Tripwire, etc.).
1		6. Changes or disables a*ll 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.*
1		7. Uses passwords that are a min. of 8 characters, expire at least annually & have complexity requirements.
1		*8. Ensures that passwords are never stored in clear text or are easily decipherable.*
1		*9. Checks all systems and software to determine whether appropriate security settings are enabled.*
1		*10. Manages file and directory permissions following least privilege and need-to-know practices.*
1	Provided by Amazon AWS	11. Implements redundancy or high availability for critical functions.
1		*12. Authenticates all user access with either a password, token or biometrics.*
1		13. Formally approves, tests and logs all system changes.
0	We use deidentified or test data, not live patient information.	14. Does not use production data for both development and testing, unless it has been declassified by the [redacted]

1		15. Uses artificial data in both development and test environments.
1		16. Limits access to development and test environments to personnel with a need to know.
2	3 failed attempts locks out a user until they sign back online. Online login attempts are monitored in our logs.	17. Sets the account lockout feature for successive failed logon attempts on all system's support computers.
0		18. Prohibits split tunneling when connecting to customer networks.
19		***Total Configuration Controls***
Answer	**Comments**	E. Product Design. The vendor:
1	AES-256 encryption	1. Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access.
1	SSL via 256-bit EV certificate	2. Ensures that access to confidential information, across a public connection, is encrypted with a secured connection and requires user authentication.
1		3. Implements protections for Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.
1		4. Audits the application against the OWASP Top 10 Application Security Risks.
1		5. Ensures that application server and database software technologies are kept up-to-date with the latest security patches.
1		6. Uses threat modeling in their software development lifecycle (SDLC).
1		7. Performs security code reviews as part of their SDLC.
1		8. Conducts OWASP code reviews for the Top 9 source code flaw categories as part of their SDLC.
8		***Total Product Design Controls***
Answer	**Comments**	F. Compliance. The vendor:
1	https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf	1. Will provide relevant certificates of applicable ISO 27001 certification.
1	FDA 510k Class II medical device / Completed 2 FDA audits to date	2. Can provide documentation that its product is HIPAA compliant, if the vendor manages any PHI on behalf of Company.
0	We do not receive any payment card data	3. Can provide documentation of its PCI-DSS compliance if the vendor manages any payment card information, on behalf of Company.
1		4. Uses industry standard best practices for application security (e.g. OWASP).
2		***Total Product Design Controls***
Answer	**Comments**	G. Access Control. The vendor:

1		1. Immediately removes, or modifies access, when personnel terminate, transfer, or change job functions.
1	Yes, for live environment. For development environment we do have shared resources for developers and testers to collaborate.	*2. Achieves individual accountability by assigning unique IDs and prohibiting password sharing.*
1		3. 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.
1		4. Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.
4		***Total Access Controls***
Answer	**Comments**	H. Monitoring. The vendor:
2	Quarterly and upon changes of employee status	1. Reviews access permissions monthly for all server files, databases, applications, etc.
1	We have web server, API, AWS, and system event logs	*2. Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.*
1		*3. Reviews and analyzes after hours system accesses, at least monthly.*
1		*4. Reviews system logs for failed logins, or failed access attempts monthly.*
1		*5. Reviews and removes dormant accounts on systems at least monthly.*
1		6. Reviews web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise.
1		7. Reviews network and firewall logs at least monthly.
0		8. Reviews wireless access logs at least monthly.
0		9. Performs scanning for rogue access points at least quarterly.
0	Can be implemented for a fee.	10. Actively manages IDS/IPS systems and alert notifications have been implemented.
1	We do not store any Company proprietary or confidential data.	11. Performs vulnerability scanning at least quarterly. This is a mandatory requirement for any system that stores Company confidential or proprietary data.
0	We do not manage any PHI on behalf of Company.	12. Performs penetration testing at least annually, if the vendor manages any PHI on behalf of Company. This is a mandatory requirement for any system that stores Company confidential or proprietary data..
1		13. Checks routinely that password complexity is adhered to.
10		***Total Monitoring Controls***
Answer	**Comments**	I. Physical Security. The vendor:

1	Amazon AWS	*1. Controls access to secure areas. E.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.*
1	Amazon AWS	*2. Controls access to server rooms and follows least privilege and need-to-know practices for those facilities.*
1	Amazon AWS	*3. Has special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.*
1		4. Shreds or incinerates printed confidential information.
1		5. Prohibits or encrypts confidential information on laptops & mobile devices.
0	Managed by hospital.	6. Positions desktops, which display confidential information, in order to protect from unauthorized viewing.
1	Amazon AWS	7. Escorts all visitors in computer rooms or server areas.
1	Amazon AWS	8. Implements appropriate environmental controls, where possible, to manage equipment risks, e.g., fire safety, temperature, humidity, battery backup, etc.
1	Amazon AWS	*9. Has no external signage indicating the content or value of the server room or any room containing confidential customer information.*
1		10. Provides an export copy of all of the customer's data in a mutually agreed upon format at the end of the contract.
1		*11. 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.*
10		***Total Physical Controls***

Answer	**Comments**	J. Contingency. The vendor:
1		1. Has a written contingency plan for mission critical computing operations.
1		2. Has emergency procedures and responsibilities documented and stored securely at multiple sites.
1		3. Reviews and updates the contingency plan at least annually.
1		*4. Has identified computing services that must be provided within specified critical timeframes, in case of a disaster.*
1		*5. Has identified cross-functional dependencies, so as to determine how the failure in one system may negatively impact another one.*
1		6. Has written backup procedures and processes.
0	Amazon	7. Tests the integrity of backup media quarterly.
0	Amazon	*8. Stores backup media in a secure manner and controls access.*
1		9. Maintains a documented and tested disaster recovery plan.
1		10. Uses off-site storage and has documented retrieval procedures for backups.

1	Amazon	11. Password protects and encrypts all backups.
1	Amazon	*12. Provides rapid access to backup data.*
0	Amazon	13. Labels backup media appropriately, to avoid errors or data exposure.
10		***Total Contingency Controls***
Answer	**Comments**	**K. Vendor's Business Associates.**
1		1. Confidentiality agreements have been signed before proprietary and/or confidential information is disclosed to the vendor's business associates.
1		2. Vendor's business associate contracts, or agreements, are in place and contain appropriate risk coverage for customer requirements.
1		3. Vendor's business associates are aware of customer security policies and what is required of them.
1		4. Vendor's business associate agreements document the agreed transfer of customer's data when the relationship terminates.
4		***Total Business Relationships Controls***
	99	***TOTAL THIRD-PARTY CONTROLS***