Surgimap

The Physician Driven Imaging Solution

A Nemaris Company

Privacy & Security Assessment

For Surgimap version 2.1.1 and higher

DATE: 12-17-2014

REVISION 1.0

306 East 15th St Suite 1R, New York NY 10003

SCREENING

Screening Questions	YES or NO
Will the system/service involve the collection of information about individuals	**No**
Will the system/service require or compel individuals to provide information about themselves?	**No**
Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?	**No**
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?	**No**
Does the system/service involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	**No**
Will the system/service result in you making decisions about individuals in ways which may have a significant impact on them?	**Yes, viewing patient images for diagnostic / direct care**
Is the information to be used about individuals' health and/or social wellbeing?	**Yes, will drive treatment decision**
Will the system/service require you to contact individuals in ways which they may find intrusive?	**No**

ASSESMENT

1. Description

Brief description *e.g. Purpose; Electronic or Paper system; For patients or staff*	Software to view/analyze medical images and determines best patient treatment for optimal care. Only to be used by surgeon & staff (medical professional) for direct care. Optional premium features allow user to share case notes & images with collaborators via our cloud solution.
IT Systems only:	
Name of supplier or in-house developer:	Company: Nemaris Inc Product: Surgimap Spine

2. Ownership

System/Information Asset Owner	Name: Nemaris Inc Title: Dept.:
System/Information Asset Administrator	Name: Title: Dept.:

3. Use of Personal Information

What data items will be held? *Tick or highlight.* None are required but other than a unique patient identifier. That said, the following can be held in Surgimap	X Name £ Address £ Post Code X Date of Birth £ Ethnic Origin £ Religion £ Sexual health X Gender £ GP Name £ Next of Kin X NHS Number £ Consultant Name X Diagnoses X Treatment information £ Medical History £ Trade Union M/ship £ National Insurance Number Other (*specify*): Patient Images
Is this information new or is it old used in a different way?	No, this is secondary to data surgeon already has in PACS / EMR system
Is there a legal or mandatory reason for using the information? *If yes, specify:*	*Yes, need to have patient images that are being analyzed for surgery tied to patient name*
Will the people whose information is held need to give their consent to the processing and disclosures that will take place?	£ Yes (implicit) £ Yes (explicit) x No
Patient systems only:	

Is the information being used for direct patient care or local audit?	Yes, patient images are analyzed for optimal surgical approach and patient care. That case plan can be shared with co-surgeons/ nurse/ others that surgeon wants to collaborate with

4. Sharing Information

Will you be receiving information in from other sources to populate your system (e.g. emails, telephone calls, electronic transfer from another system)?	*If yes provide details in Appendix 1* *Yes, from PACS, EMR, patient CD, or any other source user has available with patient images*
Will you be sending out information from the system (e.g. letters, faxes, emails, reports – electronic or paper)?	*If yes provide details in Appendix 1* Yes, emails can be sent to collaborators
Will you be sharing information with an external organisation or individual (e.g. other trusts or external providers for health care services, auditors, contractors)?	*If yes provide details in Appendix 2* No, but system user can share with external collaborators if need be i.e., not limited
Will an external organisation be processing Trust information on your behalf (e.g. to provide an managed service)	No
Will a third party be involved in supporting or maintaining trust data on the Trust's behalf e.g. IT system maintenance	No
What is the process for allowing and recording if a person wants to opt out of sharing information?	User e.g., surgeon deletes the patient record from system

5. Location & Network

Where will the information be held e.g. • *Computer system* ○ *National system – held off site secured by supplier under national T&Cs (PAS, ORMIS, PACS, RIS, Choose and Book, ESR* ○ *IT department server room governed by trust wide policies and procedures* ○ *Hosted by a third party under their network policies* • *Room/cupboard/filing cabinet*	The Surgimap software resides locally e.g., on surgeon computer. Backups can be stored on our cloud server (Amazon HIPPA compliant in USA or Europe if desired)
IT System only:	
What network will you be using? ○ *National system accessed via N3* ○ *System access via Trust network (hardwire or wireless)* ○ *UHB system access via dedicated Telewest line* ○ *Other (specify)*	Surgimap needs internet access to verify username & password and periodic updates. Any form e.g., wireless, wired works as long as connection is made to our server for verification and update downloads

6. Access to Information

Who will access the information? - *List names or staff groups*	Each Surgimap user has a personal username and password. Intended users are all Spine surgeons and their support staff e.g., Nurse, resident, fellow
How will the access be controlled *e.g.Key, Security Pass, Smartcard, Unique ID and Password, Restricted access to shared drive, Passworded file, Other – specify*	Each user has unique username & password for login and encryption
Can you differentiate between types of users and set different access levels? *If yes, give levels. If no, explain why this is not required or is not able to be done*	Yes, owner of data sets controls of who can view what information and also what they can do with that information e.g., edit or not. Some collaborators may have view only, de-identified while others have View & Edit with all patient identifiers.
How and where will you hold a list of users (active, deregistered and temporary) who access the information?	User lists are secured on our servers with their account status.
What procedures are in place for subject access requests? *i.e. if a person wants to see their data how will you manage that?*	Users login to the software with their own username and password. If they get locked out they can request a password link to be sent to the email on file

7. Audit Trail

What audit trail does the system have *e.g.* - *All changes made to the record* - *Who made the changes* - *Who has viewed the record*	Users can only see their own patient images that they loaded into Surgimap or that were shared to them as a collaborator. We track when a user signs in/out of software to view their patient images and key actions e.g., number images loaded into software, measurements applied. Also, when a collaborator has edit privileges we know who "touched" the patient record with time stamp
IT System only:	
Can you record all logons including failed attempts?	Yes, we record all logons. After 3 failed attempts the account is locked to prevent brute force entry

8. Retention & Disposal

What is the retention period for the information in this system?	The desktop software stores information indefinitely until user deletes it. If data is stored online then it is retained for 10 years post deletion for record keeping
How will the data be destroyed when no longer required?	User deletes information and it is gone from user account until retention policy expires.

9. Business Continuity

Have you got a business continuity plan Or Does your implementation plan include a work package to write a business continuity plan? *Attach the plan or give its file location*	*No, not needed. The software is freestanding medical device (CE mark) that does not need a business continuity plan. It is secondary support for surgeons. Primary patient image and data is within PACS, EMR system. Surgimap is simply a tool for image viewing, measuring, and outcome simulation*
How often will you test the business continuity plan?	*Not applicable*

10. Data Quality

Have you got a business continuity plan Or Does your implementation plan include a work package to write a business continuity plan? *Attach the plan or give its file location*	*No, not needed. The software is freestanding medical device (CE mark) that does not need a business continuity plan. It is secondary support for surgeons. Primary patient image and data is within PACS, EMR system. Surgimap is simply a tool for image viewing, measuring, and outcome simulation*
How often will you test the business continuity plan?	*Not applicable*

11. Risk Assessment

Description	**Mitigation**
Computer, laptop, medium where Surgimap resides is stolen	**Surgimap software uses 256 bit encryption**
Hacker tries to break into Surgimap with repeated username & password combinations	**User/Pwd combo must match for entry. Lockout after 3 failed attempts, user data is encrypted**
Hacker tries to crack open software	**All files are encrypted**

Appendix 1: Data Flows

Information Sent Out

Description	Surgimap allows user who has logged into their own account and views their own patient images to share the image, measurements, and case plan with others who may assist on that clinical case. Those recipients are notified by email that a case has been shared to them (no identifiers in email). The email has a link to an online site, letting recipient see the case plan or recipient starts their own Surgimap to see the case.
Who to	Any collaborator that user has shared case plan with
How sent	Electronically
Frequency	On as needed basis by user (from never to 2 cases / wk)

Information Received

Description	Surgimap can link to a PACS system via a DICOM node and import patient images (Surgimap becomes a send destination).
Who from	User logs into PACS system to see original patient images, and then selects Surgimap running on their hospital computer as the send destination.
How sent	Digital / electronically
Frequency	On as needed basis

Appendix 2: Information Sharing

Title/Description of Information	Surgimap can send a case plan (patient image, treatment plan) to collaborators that are within or external to hospital.
Person/ Organization sharing with	User can enter desired recipient, set their view and edit permissions as well as ability to see patient identifiers e.g., Name, NHS number. Recipient logs into their own Surgimap to see the shared case plan
Purpose:	Allows team members to be on same page regarding the surgical case (approach, implants needed, start day/time, etc)
Sharing method *Acceptable methods are:* • *Email attachment: NHS.net to NHS.net or encrypted attachment* • *Paper records: Secured in boxes/envelopes, clearly addressed and send via special delivery or courier* • *CDs/DVDs: Encrypted disk and send via recorded delivery if more than one person on the disk.* • *Upload to website: Via secure link using logon and password* • *Provide Trust log on and email*	Sharing is from one Surgimap account to another electronically through a centralized server. All users have their own username and password and can only see their own work or cases that were shared to them. The information can be viewed in Surgimap running on a computer or by logging into secure online site.
Location of Information Sharing Agreement or T&Cs	Each user can see the information sharing agreement and T&C's when they click on the appropriate links on the login page