Surgimap Business Associate Agreement: Privacy

Last updated: March 2017

User of any Nemaris Inc. ("Nemaris") products or services including but not limited to Surgimap, Surgimap Access, or Surgimap Mobile, on any platform (collectively, "Surgimap"), acknowledges that User is a "Covered Entity" and Nemaris is a "Business Associate" as defined by the standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic Clinical Health Act (the "HITECH Act"), which was enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA"). In accordance with the terms set forth in this "Privacy Agreement." Both the User of Nemaris products or services and Nemaris itself shall use all reasonable, best efforts to protect the privacy of Protected Health Information ("PHI").

1. Terms and Terminology

1.1. *Business Associate*. "Business Associate" within the context of this Agreement means Nemaris, the producer of Surgimap and other products and services.

1.2. *Covered Entity*. "Covered Entity" within the context of this Agreement means the user of Nemaris products or services (e.g., a healthcare provider, a health plan, or a healthcare clearinghouse).

1.3. *Patient*. "Patient" is hereby defined as a patient of Covered Entity.

1.4. *Patient Record*. "Patient Record" is defined as any item, collection, or grouping of information that includes PHI that is maintained, collected, used, or distributed by Provider.

1.5. *Person*. "Person" is defined as any legal entity or individual.

1.6. *Protected Health Information*. PHI means information, whether oral or recorded in any form or medium, including demographic information, that: (i) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; (ii) identifies the individual, or for which there is a reasonable basis for believing that the information can be used to identify the individual; and (iii) is accessed by Covered Entity through Provider, or is created by Covered Entity and used in conjunction with Provider's services, or is made accessible to Covered Entity by Provider and its services. PHI includes, without limitation, Electronic Protected Health Information ("ePHI") as that term is defined at 45 CFR § 160.103.

1.7. *Privacy Rule*. "Privacy Rule" shall mean the standards for Privacy of Individually Identifiable Health Information contained in 45 CFR Parts 160 and 164, Subparts A and E.

1.8. *Provider*. "Provider" within the context of this Agreement means Nemaris.

1.9. *Security Rule*. "Security Rule" refers to the Security Standards for the Protection of ePHI that is contained in 45 CFR §§ 160 and 164.

1.10. *Services Agreement*. "Services Agreement" is defined as the Nemaris Inc. Services Agreement between Provider and Covered Entity, which has an effective date of the acceptance of these terms and must be reviewed and accepted prior to using Surgimap.

1.11. *Terms*. Terms used, but not defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule and the Security Rule.

1.12. *Unsecured Protected Health Information*. "Unsecured Protected Health Information" and/or "Unsecured PHI" refer to information that is not secured through the use of a technology or methodology identified by the Secretary to render PHI unusable, unreadable and undecipherable to unauthorized users.

2. Covered Entity's Obligations.

2.1. *Covered Entity Subject to Same Standards and Same Penalties as Provider*. Covered Entity will comply with the use and disclosure provisions of the Privacy Rule and the security standards regarding administrative, physical and technical safeguards of the Security Rule. As set forth in the HITECH Act, Covered Entity will be subject to civil and criminal penalties for violation of the Privacy Rule or the Security Rule.

2.2. *Permitted Uses and Disclosures*. Covered Entity shall use or disclose PHI solely as necessary to perform the services set forth in the Services Agreement, and as permitted or required by this Privacy Agreement or as required by law.

2.3. *Safeguards*. Covered Entity shall use appropriate privacy and security measures to prevent the use or disclosure of PHI other than as permitted under this Privacy Agreement. Such measures shall include, but not be limited to: (i) implementing and maintaining appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any ePHI that it creates, receives, maintains, or transmits on behalf of Provider, as required by the Privacy Rule and Security Rule; and (ii) taking measures to ensure compliance with standards and implementation specifications with respect to the administrative, physical, and technical safeguards, as required by 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316.

2.4. *Mitigation*. If Covered Entity uses or discloses PHI in a manner other than as permitted under this Privacy Agreement, Covered Entity shall use its reasonable best efforts to mitigate the effects of the use or disclosure. These efforts shall include, but are not be limited to, ensuring that the improper use of PHI is discontinued immediately, seeking return or destruction of the improperly disclosed PHI, and ensuring that any person to whom PHI was improperly disclosed will not re-disclose such information.

2.5. *Duty to Report*. Covered Entity shall immediately notify Provider of any use or disclosure of PHI of which Covered Entity is aware that is not expressly authorized under this Privacy Agreement, whether made by Covered Entity, its employees, representatives, agents, or

subcontractors. Covered Entity shall also immediately notify Provider of any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with the system operations in an information system. Covered Entity shall provide in such notice the remedial or other actions taken to correct the unauthorized use or disclosure.

2.6. *Agents*. Covered Entity will ensure that any of its employees, agents, subcontractors, or other third parties with which Covered Entity does business are aware of and are bound to abide by Covered Entity's obligations under this Privacy Agreement.

2.7. *Access to Patient Record*. Covered Entity understands that a Patient has the right to access the PHI in its Patient Record in accordance with 45 C.F.R. § 164.524. To provide Patients with access to Patient Records held by Covered Entity, Covered Entity agrees to provide access to, or copies of, any Patient Record upon request by Provider. Provider shall request access by giving at least 48 hours notice by facsimile, telephone, or email.

2.8. *Amendments to Patient Record*. Covered Entity understands that Patient has the right to amend the PHI in his or her Patient Record under some circumstances. To provide Patients with the ability to amend PHI in Patient Records held by Covered Entity, Covered Entity agrees to make amendments to any Patient Record upon request of Provider. Covered Entity shall make such amendment within 30 days of the written request of Provider.

2.9. *Duty to Document Disclosures*.

a. Covered Entity will document each disclosure it makes of PHI to any other person, including Provider. The documentation shall include:

i. The date of the disclosure;

ii. The name of the person receiving the PHI, and, if known, the address of such person; and

iii. A brief statement of the purpose of the disclosure or, instead of such statement, a copy of the request for disclosure.

b. Notwithstanding Section 2.9(a), Covered Entity is not required to document the following disclosures:

i. Unless otherwise required by Section 2.10, disclosures made for the purpose of, or incidental to, carrying out treatment, payment, or health care operations;

ii. Disclosures made prior to April 14, 2003;

iii. Disclosures made to provide the Patient with access to its PHI under Section 2.7;

iv. Disclosures made pursuant to Patient's written authorization;

v. Disclosures required by law for national security or intelligence purposes;

vi. Disclosures to correctional institutions or law enforcement officials having lawful custody of Patient;

vii. Disclosures made as part of a limited data set;

viii. Disclosures made to persons actively involved in Patient's care; and

ix. Disclosures made for notification purposes in an emergency.

2.10. *Accounting of Disclosures*. Covered Entity understands that a Patient has the right to an accounting of disclosures of PHI. To provide Patients with such an accounting, Covered Entity will make available the documentation Covered Entity has collected in accordance with Section 2.9 upon written request of Provider. Covered Entity shall provide the accounting within 30 days of receipt of Provider's request. If disclosures were made by Covered Entity through the use of an electronic health record, the Patient has the right to receive an accounting of disclosures of personal health records made by Covered Entity for treatment, payment, and health care operations during the previous 3 years.

2.11. *Minimum Necessary*. Covered Entity represents and warrants that it will use and disclose PHI in accordance with the Privacy Rule's "minimum necessary" standards.

2.12. *Other Uses and Disclosures*. Covered Entity will not use or disclose PHI in any manner that would not be permissible under the Privacy Rule or the Security Rule if used or disclosed by Provider.

2.13. *Books and Records and Internal Practices*. Covered Entity agrees to make all internal practices, books, and records relating to the use and disclosure of PHI available to Provider or to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by Provider or the Secretary for the purposes of the Secretary determining Provider's compliance with the Privacy Rule and the Security Rule.

2.14. *Covered Entity's Obligations Regarding Unsecured Protected Health Information*. Covered Entity shall comply with the following obligations that relate to Unsecured PHI.

a. *Notification of Provider*. Covered Entity will notify Provider of any Patient whose Unsecured PHI has been, or is reasonably believed by Covered Entity to have been, inappropriately accessed, disclosed, or used. Such notification shall include the names and contact information of the Patients involved and shall be made without unreasonable delay, but in no case later than 30 days following discovery of such breach, unless delayed for law enforcement purposes.

b. *Notification of Patient*. Covered Entity will notify the Patient by first class mail or by email (if the Patient has indicated a preference to receive information by email) of any breaches of Unsecured PHI as soon as possible, but in any event, no later than 60 days following the discovery of the breach. Covered Entity will obtain Provider's approval of the form and content of the written notification before its issuance.

c. *Posting Notice of Breach*. In the event the breach involves 10 or more Patients whose contact information is out of date, Covered Entity will post a notice of the breach on the home page of its website or in a major print or broadcast media. Covered Entity will obtain Provider's approval of the form and content of the written notice before its posting.

d. *Notice to the Secretary*. If a breach involves more than 500 Patients, Covered Entity will immediately notify the Secretary. Covered Entity will obtain Provider's approval of the form and content of the written notice before its issuance.

e. *Contents of Notice*. The notices required under this Section shall include the following:

i. A brief description of the breach, including the date of the breach and the date of its discovery, if known; and

ii. ii. A description of the types of Unsecured PHI involved in the breach;

iii. iii. Steps the Patient should take to protect himself/herself from potential harm resulting from the breach;

iv. iv. A brief description of actions Covered Entity is taking to investigate the breach, mitigate losses, and protect against further breaches; and

v. v. Contact information, including a toll-free telephone number, e-mail address, website or postal address to permit Patient to ask questions or obtain additional information.

f. *Annual Report to Secretary and Maintenance of Log*. Covered Entity will submit an annual report to the Secretary of a breach that involved less than 500 Patients during the year and will maintain a written log of breaches involving less than 500 Patients.

3. Obligations of Provider.

3.1. *Notice of Privacy Practices*. To the extent that such limitation or restriction may affect Covered Entity's use or disclosure of PHI, Provider shall provide Covered Entity with a copy of its Notice of Privacy Practices, and notify Covered Entity of:

a. Any limitation(s) in its Notice of Privacy Practices;

b. Any changes in, or revocation of, permission by a Patient to use or disclose PHI; and

c. Any restriction to the use or disclosure of PHI to which Provider has agreed, to the extent that such restriction may affect Covered Entity's use or disclosure of PHI.

3.2. *Permissible Requests*. Provider shall not request Covered Entity to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if used or disclosed by Provider.

4. Term and Termination.

4.1. *Term*. The Term of this Privacy Agreement shall be effective as of the effective date of the Services Agreement and shall continue to be in effect until all obligations of the parties have

been met, unless terminated by mutual agreement of the parties or as provided elsewhere in this Section 4.

4.2. *Termination for Cause*. Provider may immediately terminate this Privacy Agreement and the Services Agreement if, after providing Covered Entity written notice of the existence of a material breach of this Privacy Agreement, Covered Entity fails to, or is unable to, cure the breach upon mutually agreeable terms within 10 days.

4.3. *Effect of Termination*.

a. Except as provided in Section 4.3(b), upon expiration or termination of the Services Agreement for any reason, Covered Entity shall return or destroy all PHI, including PHI that is in the possession of subcontractor or agents of Covered Entity. Covered Entity shall retain no copies of PHI.

b. To the extent that it is not feasible for Covered Entity to return or destroy all PHI, then

i. Covered Entity's obligations under this Privacy Agreement shall continue for as long as Covered Entity maintains such PHI; and

ii. Covered Entity's further uses and disclosures of PHI shall be limited to those purposes that make it not feasible for Covered Entity to return or destroy the information for as long as Covered Entity maintains such PHI.

5. Miscellaneous Provisions.

5.1. *Notice.* Notices, requests, and other communications that are required to be in writing must be personally delivered, mailed by prepaid certified mail, return receipt requested, or sent by overnight carrier, and must be addressed as follows. Such notice shall be effective upon being mailed or personally delivered.

If to Provider:
Nemaris, Inc.
Attn: Bradley Harris
306 E. 15th St, Suite 1R
New York, NY 10003

For notices to Covered Entity, it is the Covered Entity's obligation to notify Provider of its designated recipient of Notice in writing as it pertains to this Section 5.1.

5.2. *Mutual Representation and Warranty*. Covered Entity and Provider each represents and warrants to the other that all of its employees, agents, representatives, and members of its work force, whose services may be used to fulfill obligations under this Privacy Agreement and/or the Services Agreement, are or shall be appropriately informed of the terms of this Privacy Agreement and are under legal obligation to fully comply with all provisions of this Privacy Agreement.

5.3. *Covered Entity Warranty*. To the extent required by law or regulations, Covered Entity warrants that it has implemented a Red Flags Program in accordance with the Federal Trade

Commission's Identity Theft Prevention Red Flags Rule, 16 CFR § 681.1 *et seq.*, or that it agrees to comply with Provider's Red Flags Program.

5.4. *No Third Party Beneficiaries*. Nothing express or implied in this Privacy Agreement is intended to confer, or shall confer, any rights, remedies, or liabilities upon any person other than Covered Entity and Provider.

5.5. *Effect of Assignment*. This Privacy Agreement shall be binding upon and shall inure to the benefit of Covered Entity and Provider and their respective transferees, successors and assigns, except that Covered Entity shall not have the right to assign or transfer this Privacy Agreement, or Covered Entity's rights and obligations hereunder, without Provider's prior written consent. Upon assignment or transfer of this Privacy Agreement, Covered Entity shall return or destroy all PHI in accordance with the terms set forth in Section 4.3.

5.6. *Regulatory References*. A reference in this Privacy Agreement to a section in the Privacy Rule or the Security Rule or a term defined in the Privacy Rule or the Security Rule means the section or definition as in effect or as amended.

5.7. *Amendment*. Covered Entity and Provider agree to take such action to amend this Privacy Agreement as is necessary for Provider to comply with the requirements of the Privacy Rule and the Security Rule.

5.8. *Survival*. The respective rights and obligations of Covered Entity under this Privacy Agreement shall survive the termination of this Privacy Agreement and the Services Agreement.

5.9. *Interpretation*. Any ambiguity in this Privacy Agreement shall be resolved to permit Provider to comply with the Privacy Rule and the Security Rule.

5.10. *Captions and Headings*. The captions and headings in this Privacy Agreement are included for convenience and reference only, and shall in no way be held or deemed to define, limit, describe, explain, modify, amplify or add to the interpretation, construction or meaning of, or the scope or intent of, this Privacy Agreement.

IN WITNESS WHEREOF, Provider and Covered Entity have caused the execution of this Privacy Agreement by signing below or clicking "I Agree" on the Surgimap download page.

PROVIDER (Business Associate)	COVERED ENTITY (SURGIMAP USER)
Nemaris, Inc.	_____
_____	_____
Bradley Harris	_____
General Counsel	_____