BUSINESS ASSOCIATE AGREEMENT TERMS AND CONDITIONS

1. Introduction.

The Business Associate agreement requirements set forth in the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH"), and all applicable implementing regulations, including, without limitation, the Privacy Rule (45 C.F.R. § 160 and § 164 (Subparts A and E)), the Security Rule (45 C.F.R. § 160 and § 164 (Subparts A and C)), and the Breach Notification Rule (45 CFR §§ 164.400-414) are incorporated herein. All such laws and regulations may be collectively referred to herein as "HIPAA". For the avoidance of doubt, Intuitive Surgical, Inc. is the "Business Associate" and the other party named in the underlying Agreement is "Vendor."

THE BUSINESS ASSOCIATE AGREEMENT TERMS AND CONDITIONS CONTAINED HEREIN SHALL GOVERN IN THE EVENT OF ANY CONFLICT BETWEEN THESE TERMS AND THOSE OF ANY UNDERLYING, ANCILLARY OR INCORPORATING DOCUMENT.

2. Definitions. Unless otherwise defined herein, all capitalized terms shall have the same meaning as ascribed to those terms by HIPAA. Any ambiguity herein shall be resolved to permit Intuitive Surgical to comply with HIPAA.

2.1 **"Products and Services"** shall mean those certain products and/or services provided by Vendor, that require access to or use, maintenance or transmission of PHI by Vendor on behalf of Intuitive Surgical.

2.2 "**Protected Health Information**" or "**PHI**" shall have the same meaning as ascribed in 45 C.F.R. §160.103. As may be applicable, PHI shall include "Electronic Protected Health Information" or "EPHI".

2.3 "**Underlying Agreement(s)**" shall mean any written agreements, supplements, or addendums that the Parties have entered into, or will enter into, for the provision of Products and Services. This Agreement shall not be incorporated into any agreement, supplement, or addendum that does not reference this Agreement.

2.4 "**Notices."** All notice or other communication required or permitted under this Agreement shall be made in writing, and shall be deemed received five (5) business days after the date of mailing, one (1) business day after dispatch by overnight courier service or electronic mail, upon receipt if personally delivered, or upon confirmation of confirmed transmission if by facsimile. Any notice or communication shall be delivered to the respective Party, as follows:

If to Intuitive Surgical:	**If to Vendor:**
Attn: Legal – Privacy and Data Protection Group Intuitive Surgical, Inc. 1020 Kifer Road Sunnyvale, CA 94086	[Attn] [Sub-Contractor Name] [Address] [City, State ZIP]
With a copy to: Data.privacy@intusurg.com Email Subject: "BAA or HIPAA Notice"	With a copy to: [Email Address] [Misc.]

2.5 **"Relationship of the Parties"** The Parties agree Vendor is an independent contractor of Intuitive Surgical and is therefore not an agent of Intuitive Surgical. This Agreement is intended to apply only to the Parties, and nothing herein is intended for the benefit of any third party.

3. Permitted Uses and Disclosures of PHI.

3.1 **General.** Vendor shall use or disclose PHI only as permitted or required by this Agreement or the Underlying Agreement, or Intuitive Surgical, or as required by law.

3.2 **Proper Management and Administration.** Vendor may use or disclose PHI for its proper management and administration or to carry out Vendor's legal responsibilities. However, Vendor may only use or disclose PHI under this Section 3.2 to the extent that:

a. Such Uses or Disclosures are Required by Law, or

b. Vendor obtains reasonable assurances from the person to whom the information is disclosed that the person: (1) will hold the PHI confidentially and further Use or Disclose the PHI only (i) as permitted or required by law, or (ii) for

the purpose for which it was disclosed to the person; and (2) will notify Vendor of any instance the person becomes aware of in which the confidentiality of the information has been breached.

3.3 **Data Aggregation.** If requested by Intuitive Surgical, Vendor may provide Data Aggregation services relating to the health care operations of Intuitive Surgical, as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

3.4 **Data De-Identification.** Vendor may use PHI to create de-identified health information on Intuitive Surgical's behalf in accordance with 45 C.F.R. §164.514 and when specifically authorized by Intuitive Surgical in writing.

3.5 **Offshore PHI Prohibition.** Without express written consent from Intuitive Surgical, Vendor shall not and shall ensure that its agents or subcontractors shall not, access, use, disclose, transmit, create or maintain any PHI outside of the United States.

3.6 **Marketing/Fundraising/Sale of PHI.** Vendor shall not use or disclose PHI for purposes of marketing or fundraising. Vendor shall not sell PHI or otherwise receive remuneration, directly or indirectly, in exchange for PHI; provided however, that this prohibition shall not affect payment to Vendor by Intuitive Surgical for performance of services set forth in the Underlying Agreement.

4. Vendor Obligations.

4.1 **General.** Vendor shall not use or disclose PHI other than as permitted or required by this Agreement or the Underlying Agreement, or as required by law.

4.2 **Safeguards.** Vendor shall implement reasonable and appropriate Administrative, Physical, and Technical safeguards to ensure the Confidentiality, Integrity, and Availability of EPHI, to prevent Use or Disclosure of the PHI other than as provided for by this Agreement or the Underlying Agreement.

4.3 **Minimum Necessary.** Vendor shall Use or Disclosure only the Minimum Necessary PHI to accomplish the intended purpose of the Use or Disclosure.

4.4 **Security Incidents.** In the event Vendor discovers the occurrence of any successful Security Incident, Vendor shall, within five (5) days of discovery of such successful Security Incident, notify Intuitive Surgical of the same. The Parties acknowledge the ongoing existence and occurrence of attempted but "Unsuccessful Security Incidents". Unsuccessful Security Incidents shall include pings, and other surveillance activities on Vendor's firewall, port scans, unsuccessful log on attempts and password-based attacks, denials of service attempts, other common firewall attacks, and any combination of the above so long as no such incident results in a successful Security Incident.

4.5 **Impermissible Uses and Disclosures.** In the event Vendor discovers the occurrence of any impermissible Use or Disclosure of PHI by it, Vendor shall, within five (5) days of discovery of such impermissible Use or Disclosure, notify Intuitive Surgical of the same.

4.6 **Breaches of Unsecured PHI.** In the event Vendor discovers the occurrence of its Breach of Unsecured PHI ("Breach"), Vendor shall, within three (3) business days of discovery of such Breach, notify Intuitive Surgical of the Breach. The notification to Intuitive Surgical shall include all information required by 45 CFR § 164.410(c) to the extent then known. If the information required is not available to Vendor at the time of the notification, Vendor shall thereafter provide supplemental information to Intuitive Surgical as soon as possible.

4.7 **Indemnification for Breach.** Vendor agrees to indemnify and hold harmless Intuitive Surgical and any Intuitive Surgical affiliate, officer, director, employee or agent from and against any claim, cause of action, liability, damage, fine or penalty, settlement or resolution agreement, cost or expense (including reasonable attorneys' fees), or court costs, arising out of or in connection with a Breach by Vendor or any subcontractor, agent, person or entity contracted by or under the control of Vendor (collectively "Claim"). This section is applicable whether or not Vendor has insurance coverage for such indemnification. This section shall survive termination of this Agreement, and any Claim is without regard to any limitation or exclusion of damages or other liability provision otherwise set forth in the Underlying Agreement or any availability of insurance coverage.

4.8 **Mitigation.** Vendor shall mitigate any harmful effect known to Intuitive Surgical of any successful Security Incident, impermissible Use or Disclosure of PHI, or Breach of Unsecured PHI.

4.9 **Subcontractors.** Vendor shall ensure that any of its subcontractors that access, create, maintain, or transmit PHI for or on behalf of it agree to restrictions and conditions at least as stringent as those that apply to Vendor under these this Agreement.

4.10 **Designated Record Sets.** To the extent Vendor maintains any PHI in a Designated Record Set, the following shall apply:

a. **Access to PHI.** Upon Intuitive Surgical's written request to Vendor, Vendor agrees to provide Intuitive Surgical with a copy of an Individual's PHI maintained in a Designated Record Set within twenty (20) business days of such request. Vendor shall provide such copy in the manner required by law. In the event an Individual submits a request directly to Vendor to provide a copy of PHI maintained in a Designated Record Set, Vendor shall notify Intuitive Surgical of the request within twenty (20) business days to allow Intuitive Surgical to respond to the Individual.

b. **Amendment to PHI.** Upon Intuitive Surgical's written request to Vendor, Vendor shall amend the Individual's PHI maintained in a Designated Record Set within twenty (20) business days of such request. In the event an Individual submits a request directly to Vendor to amend PHI maintained in a Designated Record Set, Vendor shall notify Intuitive Surgical of the request within twenty (20) business days to allow Intuitive Surgical to respond to the Individual.

4.11 **Accounting of Disclosures.** Upon Intuitive Surgical's written request to Vendor, Vendor agrees to provide Intuitive Surgical with an accounting of Disclosures of the Individual's PHI, as well as any information required by 45 C.F.R. § 164.528, within twenty (20) business days of such request, to allow for Intuitive Surgical to make the accounting to the Individual. In the event an Individual submits a request directly to Vendor for an accounting of Disclosures of the Individual's PHI, Vendor shall notify Intuitive Surgical of the request within twenty (20) business days to allow Intuitive Surgical to respond to the Individual.

4.12 **Audits.** Vendor shall make its internal practices, books, and records relating to the Use and Disclosure of PHI available to Intuitive Surgical and/or the Secretary for purposes of determining the Parties' compliance with applicable law or regulation.

4.13 **Compliance with Laws.** Vendor shall comply with all applicable laws and regulations that apply to individually identifiable health information. To the extent Vendor is to carry out an obligation of Intuitive Surgical, as may be required by law, Vendor agrees to comply with the requirements of the applicable law in the performance of such obligation.

5. Intuitive Surgical Obligations.

5.1 **Notice to Vendor.** To the extent Vendor's ability to Use or Disclose PHI is impacted, Intuitive Surgical shall notify Vendor of any: (i) limitation in Intuitive Surgical's notice of privacy practices; (ii) changes to, or revocation of, an Individual's permission to Use or Disclose PHI; or (iii) restriction to the Use or Disclosure of PHI that Intuitive Surgical has agreed to.

5.2 **Minimum Necessary.** Intuitive Surgical shall provide to Vendor only the Minimum Necessary PHI to accomplish the intended purpose of the Use or Disclosure.

6. Term and Termination.

6.1 **Term.** This Agreement shall commence as of the Effective Date, and shall continue until termination, as described below in Section 6.2 ("Termination"). Such termination shall be in accordance with the provisions set forth below in Section 6.3 ("Effect of Termination").

6.2 **Termination.** Upon determination that either Party has breached a material term of this Agreement, the non-breaching Party shall provide the breaching party with written notice of the existence of the alleged breach and afford the breaching party an opportunity to cure upon mutually agreeable terms. If, after meeting in good faith, the Parties cannot agree upon a cure to the alleged breach, this Agreement may be terminated by the non-breaching Party upon thirty (30) days' written notice. Further, upon written notice by either Party, this Agreement will terminate upon the termination of, or expiration of, the final Underlying Agreement in effect between the Parties.

6.3 **Effect of Termination.** Upon termination of this Agreement, Vendor shall return or destroy all PHI it maintains in any form, and shall retain no copies of such PHI. To the extent the return or destruction of PHI is not feasible, Vendor shall provide Intuitive Surgical with the reasons that make return or destruction infeasible (including an estimate of the duration of infeasibility) and extend the protections of this Agreement to the PHI retained by Vendor, and shall limit further Use or Disclosure to those purposes that make the return or destruction of the PHI infeasible. To the extent that Vendor maintains any PHI of Intuitive Surgical beyond such termination, the obligation shall remain in full force and effect as required for the protection of the privacy, security and integrity of the PHI. Any provision of these terms which by nature requires survival shall survive termination of this Agreement.