Business Associate Agreement

For purposes of this Business Associate Agreement (BAA), the Supplier shall be hereinafter referred to as "**Business Associate**."

1. Background

Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, as amended by the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005, Part I, Title XIII, Subpart D, Sections 13401-13409, (the "**HITECH Act**"), (collectively, "**HIPAA**") provides that Supplier comply with standards to protect the security, confidentiality, and integrity of health information; and

The U. S. Department of Health and Human Services has issued regulations under HIPAA (the "**HIPAA Regulations**"), including the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, sub-parts A and E, as amended by the HITECH Act (the "**Privacy Rule**") and the Standards for Security of Electronic Protected Health Information, 45 CFR Parts 160, 162 and 164, as amended by the HITECH Act (the "**Security Rule**") (collectively, the "**Privacy and Security Rules**"); and

Sections 164.502(e) and 164.504(e) of the Privacy and Security Rules set forth standards and requirements for Cisco to enter into written agreements with certain business associates that will have access to Protected Health Information (as defined below); and

Business Associate will provide Services under the Agreement as a subcontractor to Cisco on behalf of a Covered Entity (as defined in the Privacy and Security Rules).

2. Definitions

2.1. "**Breach**" shall have the meaning given to such term in 45 CFR Section 164.402.

2.2. "**Designated Record Set**" shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.

2.3. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall mean Protected Health Information which is transmitted by Electronic Media (as defined in the Privacy and Security Rules) or maintained in Electronic Media.

2.4. "**Individual**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

2.5. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103, limited to the information created or received by Business Associate from or on behalf of Cisco. "Protected Health Information" includes, without limitation, "Electronic Protected Health Information."

2.6. "**Required by Law**" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103.

2.7. "**Secretary**" shall mean the Secretary of the U. S. Department of Health and Human Services or his or her designee.

2.8. "**Security Incident**" shall have the meaning given to such term under the Security Rule at 45 CFR Section 164.304.

2.9. "**Service**" or "**Services"** means a service offering from Supplier described in an applicable service or offer description, statement of work, or purchase order listed selected by Cisco.

3. Permitted Uses and Disclosures of PHI. Business Associate shall not use or further disclose PHI other than as permitted or required by this BAA or as otherwise Required by Law. In connection with the foregoing and except as otherwise limited in this BAA, Business Associate may:

3.1. Use or disclose PHI to perform functions, activities, or Services for, or on behalf of, Cisco that are necessary to Perform under the Agreement or applicable SOW, provided that such use or disclosure would not violate the Privacy and Security Rules if performed by Cisco;

3.2. Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and

3.3. Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Responsibilities of Business Associate

4.1. **Appropriate Safeguards.** Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAA. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule. In furtherance of compliance with such requirements, Business Associate shall:

a. maintain an information security program that meets or exceeds the level required by the HIPAA Security Rule;

b. maintain policies and procedures for Business Associate's organization, consistent with the HIPAA Privacy and Security Rules and shall identify an individual within the Business Associate's organization who is responsible for enforcement and oversight of such privacy and security policies and procedures;

c. ensure that any and all employees of Business Associate that handle or access PHI undergo ongoing training regarding the safeguarding of PHI;

d. ensure that any and all third parties that access Covered Entity's confidential data or PHI with whom Business Associate contracts or relies upon for the provision of Services also maintain a framework for compliance with the HIPAA Privacy and Security Rules;

e. implement a contingency plan for responding to emergencies and/or disruptions to business that in any way affect the use, access, disclosure or other handling of Covered Entity's data and PHI;

f. maintain and exercise a plan to respond to internal and external security threats and violations, including an incident response plan;

g. maintain policies and procedures that specifically address how security breaches that are identified will be addressed;

h. maintain technology policies and procedures that provide reasonable safeguards for the protection of PHI on hardware and software utilized by Business Associate;

i. ensure that the electronic transmission of PHI is encrypted meeting at least the minimum standards required by Cisco's data security policies and applicable National Institute of Standards and Technology guidelines.

4.2. **Security Survey.** During the term of this BAA, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Cisco in understanding and documenting Business Associate's security procedures and compliance with the requirements contained herein.

Business Associate's failure to complete either of these documents within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement.

4.3. **Additional Information.** Business Associate shall provide Cisco with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Cisco may from time-to-time request. Failure of Business Associate to complete or to respond to Cisco's request for information within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement. If Cisco has reasonable concern regarding compliance with the terms of this BAA or the occurrence of a breach, Cisco will be granted access to facilities in order to review policies, procedures and controls relating to the compliance with the terms of this BAA.

4.4. **Reporting of Improper Use or Disclosure.** Business Associate shall promptly report to Cisco any use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of Unsecured Protected Health Information (as defined in the Privacy and Security Rules). In addition, Business Associate shall promptly report to Cisco any Security Incident. If Cisco determines that such use or disclosure may constitute a Breach of Unsecured Protected Health Information, Business Associate agrees to provide Cisco written notification of the Breach that includes the following information within three (3) days: (1) a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach; (2) the identification of each individual whose Unsecured PHI was breached; (3) a description of the types of Unsecured PHI that were involved in the Breach; (4) any steps individuals should take to protect themselves from potential harm resulting from the Breach; and (5) a brief description of actions that Business Associate is undertaking to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches.

4.5. **Business Associate's Agents.** Business Associate shall ensure that any agent, including a subcontractor, to whom it provides any PHI received from Cisco agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such PHI.

4.6. **Access to PHI.** At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make available PHI in a Designated Record set to Cisco as necessary to meet the requirements under 45 CFR Section 164.524.

4.7. **Amendment of PHI.** At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make any amendment(s) to PHI maintained in a Designated Record Set pursuant to 45 CFR Section 164.526.

4.8. **Documentation of Disclosures.** Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

4.9. **Accounting of Disclosures.** Business Associate agrees to provide to Cisco, in the reasonable time and manner designated by Cisco, information collected in accordance with Section 3.8 (Documentation of Disclosures) of this BAA, to permit Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

4.10. **Governmental Access to Records.** Business Associate shall make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Cisco available to the Secretary for purposes of the Secretary determining Cisco's compliance with the Privacy and Security Rules.

5. **Responsibilities of Cisco.** In addition to any other obligations set forth in this BAA, Cisco shall:

   5.1. provide to Business Associate only the minimum PHI necessary to accomplish the Services;

   5.2. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI, as required by the Security Rule; and

   5.3. obtain any consent or authorization that may be required by applicable or federal or state laws and regulations prior to furnishing PHI to Business Associate.

6. **Term and Termination.** The term of this BAA shall commence as of the Effective Date and continue coterminous with the Agreement unless otherwise terminated as set forth herein. Upon Cisco's knowledge of a material breach by Business Associate of this BAA, Cisco shall either (i) provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Cisco, or (ii) immediately terminate this BAA if cure is not possible. Upon termination of this BAA for any reason, Business Associate shall return or destroy all PHI received from Cisco, or created or received by Business Associate on behalf of Cisco, and shall retain no copies of PHI. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Cisco notification of the conditions that make return or destruction infeasible. If Business Associate determines that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. **Regulatory References.** A reference in this BAA to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

8. **No Agency Relationship.** Each Party shall maintain its own independent HIPAA and HITECH Act compliance obligations. The Parties will provide their services as separate legal entities and independent contractors. The Parties expressly agree that no agency relationship is created by this BAA or the underlying Agreement with regard to the individual Parties' HIPAA obligations. Each Party certifies that (1) Cisco shall not have the right or authority to control Business Associate's conduct in the performance of services or in the performance of HIPAA obligations; (2) Cisco shall not have the authority to direct the daily performance of services by Business Associate; and (3) Cisco shall not have the right to give interim instruction to Business Associate regarding the performance of services.

9. **Interpretation.** Any ambiguity in this BAA shall be resolved to permit Cisco to comply with the Privacy and Security Rules.