CONFIDENTIALITY AND PRIVACY AMENDMENT

This Confidentiality and Privacy Amendment (this "Amendment"), is made part of and incorporated into the Special Agent Agreement between Special Agent and Company (the "Agreement"), and is effective on the effective date of the Agreement. This Amendment supersedes and replaces in its entirety all prior versions of this Amendment. If there are any inconsistencies between this Amendment and the Agreement, the terms of this Amendment shall control.

1. **Definitions**. The following terms shall have the following meanings:

(a) ***"Business Information"*** means information, which relates to customers or the business of Company including without limitation, sales and rate information, software, business plans and operating strategies, Product information, and material identifying an association with the Company. Business Information shall not include any information that (i) relates to direct or indirect compensation payable, paid or provided to Special Agent under the Agreement; (ii) is or becomes part of the public domain or is publicly available through no act or omission or through no breach of any contract; (iii) is known at the time of disclosure without an obligation to keep it confidential, as evidenced by documentation in possession at the time of such disclosure; (iv) becomes rightfully known from another source without restriction on disclosure or use; or (v) has been independently developed without the use of or any reference to Business Information.

(b) "***Confidential Information***" means Business Information and Personal Information created by or received from the other party on behalf of Company.

(c) "***HIPAA Privacy and Security Rules***" means the Privacy, Security and Breach Notification and Enforcement Rules at 45 CFR part 160 and part 164, as may be amended from time to time.

(d) "***Information Security Breach***" means the unauthorized acquisition, access, use, disclosure, transmittal, storage or transportation of Confidential Information which is not permitted by law or by the terms of this Amendment, including, but not limited to, a Security Incident.

(e) "***Personal Information***" means a first name or initial, and last name, in combination with any demographic, medical or financial information such as age, gender, address, Social Security number, past, present or future physical or mental health condition or treatment, debt status or history, income and other similar individually identifiable personal information that is not publicly available or that has been designated as such by law or regulation. The term "Personal Information" includes, but is not limited to, Protected Health Information.

(f) "***Protected Health Information***" shall have the same meaning as that assigned in the HIPAA Privacy and Security Rules limited to the information created or received from or on behalf of Company.

(g) "***Representatives***" means all directors, officers, employees, agents, consultants, Subcontractors, professional advisors and affiliates of Special Agent.

(h) ***"Security Incident"*** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operation, in an electronic information system containing Confidential Information.

(i) ***"Subcontractors"*** means all persons to whom Special Agent delegates a function, activity or service under the Agreement, other than in the capacity of a member of the workforce of Special Agent.

2. **Special Agent's Obligations Regarding Confidential Information**. The performance of the duties and obligations required under the Agreement may require either party to disclose to the other certain Confidential Information.

(a) ***Confidentiality***. Special Agent agrees to retain all Confidential Information in confidence, and shall not use, disclose, transmit, store or transport the Company's Confidential Information except as allowed under this Amendment and for purposes related to the performance of obligations under the Agreement. Special Agent is responsible to Company for a breach of the terms of this Amendment and for any Information Security Breach by itself or its Representatives.

(b) ***Reporting an Information Security Breach or Successful Security Incident***. Special Agent agrees to report to Company any Information Security Breach and any successful Security Incident of which it becomes aware. Any report made pursuant to this Section 2(b) shall be made as soon as possible, but in no event later than five (5) business days following the date that Special Agent becomes aware of the Information Security Breach or successful Security Incident. Special Agent shall take action(s) requested by Company to document and mitigate the Information Security Breach or successful Security Incident. Special Agent shall cooperate in evaluating the necessity of providing any and all notices of an Information Security Breach or successful Security Incident as deemed advisable or as otherwise required under applicable laws or regulations.

(c) ***Return of Confidential Information***. During the term of the Agreement, Special Agent shall only retain Confidential Information which is necessary to continue proper management and administration of the services under the Agreement, or to carry out its legal responsibilities. Upon termination of the Agreement, Special Agent shall return, or if agreed to by Company, destroy all Confidential Information that Special Agent maintains in any form. Should Confidential Information be maintained beyond the termination of the Agreement for legitimate business purposes or as may be required by law, then Special Agent shall limit the use, disclosure, transmittal, storage or transportation of Confidential Information to the specific reason requiring retention of Confidential Information, and the protections of the Agreement and this Amendment shall be extended for so long as Confidential Information is maintained. Once the reason

for retention of Confidential Information has expired Confidential Information will be returned or, if agreed to by Company, destroyed.

(d) ***Disposal of Confidential Information***. Special Agent agrees to maintain a security policy for the disposal of paper and any other media that contains Confidential Information that includes a technology or methodology that will render Confidential Information unusable, unreadable or indecipherable.

(e) ***Cost of an Information Security Breach***. Special Agent shall pay Company all costs or expenses that result from Special Agent's acts or failure to act that result in an Information Security Breach.

3. **Permitted Uses and Disclosures by Special Agent**. Unless otherwise prohibited by the Agreement, this Amendment or applicable laws or regulations, including the HIPAA Privacy and Security Rules, Special Agent may use, disclose, transmit, store and transport Confidential Information:

(a) for the proper management and administration of Special Agent's business, provided that the use, disclosure, transmittal, storage and transportation are required by law, or Special Agent obtains reasonable assurances from the entity or person to whom the Confidential Information is disclosed that it will remain confidential and be used, disclosed, transmitted, stored, or transported only as required by law or for the purpose for which it was disclosed to the entity or person;

(b) to carry out the legal responsibilities of Special Agent;

(c) to its Representatives if the Representatives are first informed of the confidential nature of such information and the obligations set forth herein, and agree to be bound thereby; and

(d) to its Subcontractors if Subcontractors have entered into a written agreement with Special Agent under which Subcontractors agree to be bound by the obligations in this Amendment.

4. **Special Agent's Additional Obligations Regarding Protected Health Information**. Special Agent acknowledges that it is subject to the following requirements to the same extent as applicable to Company:

(a) to comply with subpart C of 45 CFR part 164 of the HIPAA Privacy and Security Rules, requiring development, implementation, maintenance and use of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information, that it creates, receives, maintains or transmits on behalf of Company;

(b) at the request of and in the time, manner and means, electronic or otherwise, as specified by Company, to provide access to Protected Health Information to

Company, or to an individual as directed by Company, in order to meet the requirements of the HIPAA Privacy and Security Rules;

(c) to make any amendment(s) to Protected Health Information that Company directs or agrees to pursuant to HIPAA Privacy and Security Rules in the time and manner designated by Company;

(d) to document and maintain information on any disclosure of Protected Health Information for at least six (6) years, and upon request, in the time, manner and means designated by Company, make any information about the disclosure of Protected Health Information available to Company or to an individual as directed by Company, in order for Company to meet the accounting requirements of the HIPAA Privacy and Security Rules;

(e) to make Protected Health Information and its internal practices, books and records, including policies and procedures, relating to the use and disclosure of Protected Health Information, available to the Secretary of Health and Human Services or to a state Attorney General for purposes of determining Special Agent's or Company's compliance with the HIPAA Privacy and Security Rules; and

(f) upon written request of Company, to provide Company a report of Security Incidents of which it becomes aware that are attempted but not successful.

5. **General Security Requirements**.

(a) Special Agent shall have a written, comprehensive information security program for the establishment and maintenance of a security system covering all electronic equipment, including its computers and any wireless system that, at a minimum, has the following elements:

(i) Secure user authentication protocols that include:

(A) control of user IDs and other identifiers;

(B) a secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(C) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(D) restricting access to active users and active user accounts only;

(E) blocking access to user identification after multiple unsuccessful attempts to gain access or limitation placed on access for the particular system;

(F) prohibitions against sharing or migrating access privileges to another individual; and

(G) assignment of access privileges only to identifiable, individual accounts, and all activity conducted by these accounts must be auditable.

(ii) Secure access control measures that:

(A) restrict access to records and files containing Confidential Information to those who need such information to perform their job duties; and

(B) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

(b) Company may require Special Agent to have an annual review and/or an annual technical audit of its security policies and practices by Company, or, at Special Agent's option and expense, an independent auditor, to ensure compliance with this Amendment. The third party audit report, including recommendations for remedying deficiencies where appropriate, will be provided to Company within seven (7) business days of receipt of the report by Special Agent. Special Agent shall have thirty (30) calendar days to implement remedies to any identified deficiencies, and notify Company that such deficiencies have been addressed. Special Agent's failure to remedy the identified deficiencies shall be considered in breach of this Section 5.

(c) Special Agent will encrypt all records and files containing Confidential Information that are transmitted across public networks or transmitted wirelessly.

(d) Special Agent will encrypt all desktop computers, laptops and all other portable devices on which Confidential Information is stored.

(e) Special Agent will monitor systems for unauthorized use of or access to Confidential Information.

(f) For files containing Confidential Information on a system that is connected to the Internet, Special Agent will maintain up-to-date firewall protection and operating system security patches designed to maintain the integrity of the Confidential Information.

(g) Special Agent will maintain up-to-date versions of system security agent software which includes malware protection and up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(h) Special Agent will educate and train employees on the proper use of the computer security system and the importance of Confidential Information security. In addition:

(i) Special Agent will designate one or more employees to maintain the comprehensive information security program.

(ii) Special Agent will identify and assess foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing Confidential Information, and will evaluate and improve, where necessary, the effectiveness of their current safeguards for limiting such risks, including but not limited to: (A) ongoing employee (including temporary and contract employee) training; (B) employee compliance with policies and procedures; and (C) means for detecting and preventing security system failures.

(iii) Special Agent will maintain a security policy for Representatives that protects records containing Confidential Information that are transported outside of business premises.

(iv) Special Agent will impose appropriate disciplinary measures for employees that violate its comprehensive information security program rules.

(v) Special Agent will have processes in place to prevent terminated employees from accessing records containing Confidential Information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

(i) No transfer of Confidential Information may be made by Special Agent outside of the United States without the prior, express written authorization of Company.

6. **PCI-DSS Requirements for Special Agent**. If Special Agent stores or transmits credit or debit card data, it will employ safeguards that comply with the Payment Card Industry Data Security Standard (PCI-DSS), as may be amended from time to time.

7. **General Provisions**.

(a) ***Compliance with Laws***. Special Agent shall comply with its obligations under this Amendment and with any laws or regulations as may now be in effect or as may hereafter be enacted, adopted or determined that apply to the confidentiality, use, disclosure, transmittal, storage or transportation of Confidential Information.

(b) ***Amendment***. This Amendment shall be amended to conform to any new or different legal requirements that result from any changes, revisions or replacements of any laws or regulations as may now be in effect or as may hereafter be enacted, adopted or determined that apply to the confidentiality, use, disclosure, transmittal, storage or transportation of Confidential Information,

including, without limitation, the HIPAA Privacy and Security Rules, on or before effective compliance date thereof. Company may change, revise or replace this Amendment in its sole discretion upon notice to Special Agent without the consent of Special Agent. In the event of a conflict between the requirements of this Amendment and those of the HIPAA Privacy and Security Rules, the HIPAA Privacy and Security Rules shall control. Any such amendment will automatically be effective upon the effective compliance date of such laws or regulations and shall become effective upon without the signature of either party.

(c) ***Termination for Cause***. In addition to any other termination provisions contained in the Agreement, a party may terminate the Agreement upon written notice to the other party that they have breached a term of this Amendment.

(d) ***Disclosures Required By Law or a Governmental Authority***. If Special Agent is required to disclose Company's Confidential Information in response to legal process or a governmental authority, Special Agent shall immediately notify Company and, upon request, cooperate with Company in connection with obtaining a protective order. Special Agent shall furnish only that portion of Confidential Information which it is legally required to disclose and shall use commercially reasonable efforts to ensure that Confidential Information is treated confidentially.

(e) ***Indemnification***. Notwithstanding any other provisions of the Agreement, Special Agent shall indemnify, defend and hold Company, its affiliates, directors, officers and employees, harmless for any liabilities, claims, demands, suits, losses, damages, costs, obligations and expenses, including without limitation attorneys' fees, court costs and punitive or similar damages, incurred by Company which result from any breach of this Amendment by Special Agent.

(f) ***Equitable Relief***. Special Agent acknowledges that Confidential Information it receives is confidential and/or proprietary to Company, that disclosure thereof could be seriously harmful to the business prospects of Company, that Company may not have adequate remedies at law for a breach of the confidentiality obligations hereunder and that money damages may be difficult or impossible to determine. Accordingly, Special Agent agrees, in addition to all other remedies available at law, that, in the event of a breach or threatened breach of this Amendment, Company shall be entitled to (i) seek and obtain equitable relief, including injunctive relief, and (ii) reimbursement of all attorneys' fees and court costs arising in connection with seeking and obtaining such equitable relief.

(g) ***Material Obligation/Survival***. Each obligation contained in this Amendment is deemed to be a material obligation of the parties hereunder and shall survive the termination of the Agreement.

(h) ***Interpretation***. In the event of an inconsistency or conflict between the terms of the Agreement and the terms of this Amendment, this Amendment shall control. Any such inconsistency or conflict shall be resolved in favor of a meaning that

permits the parties to comply with the HIPAA Privacy and Security Rules or any other laws or regulations that apply to the confidentiality of Personal Information. This provision shall supersede any similar provision in the Agreement. In the event of an inconsistency between the provisions of this Amendment and mandatory provisions of the HIPAA Privacy and Security Rules or any other laws or regulations that apply to the confidentiality of Personal Information, as may be amended from time to time, the HIPAA Privacy and Security Rules or any other laws or regulations that apply to the confidentiality of Personal Information, including, without limitation, any definitions in any such laws or regulations, shall control. Where provisions of this Amendment are different than those mandated in the HIPAA Privacy and Security Rules or any other laws or regulations that apply to the confidentiality of Personal Information, but are nonetheless permitted by such laws or regulations, the provisions of this Amendment shall control.