CONFIDENTIALITY AND SECURITY AMENDMENT
PRODUCER AGREEMENT

This Confidentiality and Security Amendment (this "Amendment") is made part of and incorporated into the Producer Agreement between Producer and Company ("Agreement") and is effective on the later of March 1, 2011 or the effective date of the Agreement. This Amendment revokes and replaces in its entirety any prior Confidentiality and Privacy Amendment made a part of and incorporated into the Agreement. To the extent any provisions of the Agreement conflict with or are inconsistent with any provisions of this Amendment, the provisions of this Amendment shall control. All other terms and conditions of the Agreement not inconsistent with the terms of this Amendment shall remain in full force and effect.

1. Definitions. Except as otherwise defined, any and all capitalized terms in this Amendment shall have the definitions set forth in the Agreement.

(a) "*Business Information*" means the following nonpublic business or financial information whether in written, oral or electronic form: 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 does not include (i) information similar to Business Information which is independently owned and developed by Producer or (ii) information relating to direct or indirect compensation payable, paid or provided to Producer under the Agreement.

(b) "*Confidential Information*" means Business Information and Personal Information.

(c) "*HIPAA Privacy and Security Rules*" means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and 164 and the Security Standards at 45 CFR part 160, part 162 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 or present physical and mental health condition and treatment, debt status or history, income and other similar individually identifiable personal information which is not publicly available. 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 Producer.

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

2. Producer's Obligations Regarding Confidential Information.

(a) *Confidentiality*. Producer agrees to retain all Confidential Information in strict confidence. Producer will not use, disclose, transmit, store or transport Confidential Information except for purposes related to Producer's performance of obligations under the Agreement. Producer is responsible to Company for any Information Security Breach by its Representatives.

(b) Reporting Unauthorized Use, Disclosure or Information Security Breach. Producer agrees to report each of the following to Company:

(i) any use, disclosure or Information Security Breach of Confidential Information not authorized or provided for by the Agreement; and

(ii) 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 three (3) business days following the date that Producer becomes aware of such unauthorized use, disclosure, Information Security Breach or successful Security Incident. Producer shall take action(s) requested by Company to mitigate any such unauthorized use, disclosure, Information Security Breach or Security Incident.

(c) *Return of Confidential Information*. Producer will promptly return or destroy all Confidential Information and retain no copies of it (i) upon termination of the Agreement, for any reason; (ii) once the Confidential Information is no longer needed to perform a service under the Agreement; (iii) if the Producer is not required by law to retain the Confidential Information; or (iv) once the Confidential Information has been retained through the expiration of the Producer's record retention requirements. Upon written request of Company, the destruction or return of the Confidential Information shall be confirmed in writing. If the return or destruction of the Confidential Information is not feasible, the protections of the Agreement shall be extended for so long as Producer maintains the Confidential Information. Producer's use and disclosure of such Confidential Information shall be limited to those purposes that make the return or destruction of the Confidential Information not feasible.

(d) *Disposal of Confidential Information*. Producer 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 the Confidential Information unusable, unreadable or indecipherable.

3. Permitted Uses and Disclosures of Confidential Information by Producer. Unless otherwise prohibited by the Agreement, this Amendment or state or federal laws or regulations, Producer may use, disclose, transmit, store and transport Confidential Information:

(a) for the proper management and administration of Producer's business, provided that the use, disclosure, transmittal, storage and transportation are required by law, or Producer 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 person;

(b) to carry out the legal responsibilities of Producer; and

(c) to its Representatives if the Representative is first informed of the confidential nature of such information and the obligations set forth herein, and agrees to be bound thereby.

4. Producer's Additional Obligations Regarding Protected Health Information. Producer agrees as follows:

(a) to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Company.

(b) at the request of and in the time and manner designated by Company, to provide access to Protected Health Information to Company or, as directed by Company, to an individual in order to meet the requirements of the HIPAA Privacy and Security Rules.

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

(d) to document any disclosure of Protected Health Information and, upon request in the time and manner designated by Company, make any information about the disclosure of Protected Health Information available to Company in order for Company to meet the accounting requirements of the HIPAA Privacy and Security Rules.

(e) to make its internal practices, books and records 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 the Company's compliance with the HIPAA Privacy and Security Rules.

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

5. General Security Requirements. When storing Confidential Information, Producer shall comply with the following requirements:

(a) Producer shall have a written, comprehensive information security program for the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have 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) To the extent technically feasible, Producer will encrypt all records and files containing Confidential Information that are transmitted across public networks or transmitted wirelessly.

(c) Producer will monitor systems for unauthorized use of or access to Confidential Information.

(d) Producer will encrypt all Confidential Information stored on laptops or other portable devices.

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

(f) Producer 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.

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

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

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

(iv) Producer will impose appropriate disciplinary measures for employees that violate their comprehensive information security program rules.

(v) Producer 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.

6. PCI-DSS Requirements. Producer will not store any credit or debit card data. If Producer transmits any credit or debit card data for any reason pursuant to the terms of the Agreement or this Amendment, Producer will employ safeguards that comply with the Company's policies and the Payment Card Industry Data Security Standard (PCI-DSS), as may be amended from time to time, or otherwise protect the data by adequately securing its transmission.

7. General Provisions.

(a) *Compliance with Laws*. Producer shall comply with its obligations under the Agreement, this Amendment and under any applicable state or federal law or regulations as may be in effect or as may hereafter be enacted, adopted or determined regarding the confidentiality, use, disclosure, transmittal, storage or transportation of Confidential Information.

(b) *Amendment*. This Amendment shall be amended to conform to any legal requirements that result from any changes, revisions or replacements of any applicable state or federal law or regulation as may now be in effect or as may hereafter be enacted, adopted or determined regarding the confidentiality, use, disclosure, transmittal, storage or transportation of Confidential Information, including, without limitation, the HIPAA Privacy and Security Rules, on or before the effective date thereof. Company may change, revise or replace this Amendment in its sole discretion upon notice to Producer without the consent of Producer. 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.

(c) *Disclosures Required By Law or a Governmental Authority*. If Producer is required to disclose Confidential Information in response to legal process or a governmental authority, Producer shall immediately notify Company and, upon request, cooperate with Company in connection with obtaining a protective order. Producer shall furnish only that portion of the Confidential Information which it is legally required to disclose and shall use commercially reasonable efforts to ensure that confidential treatment shall be accorded such Confidential Information.

(d) *Survival*. The respective rights and obligations of Producer under this Amendment shall survive the termination of the Agreement.

(e) *Cost of an Information Security Breach*. Producer shall be responsible for the costs associated with an Information Security Breach that results from the failure of Producer's information security program or Producer's failure to comply with federal or state laws. Producer will cooperate with Company to mitigate any damages that may result.

(f) *Termination for Violation of this Amendment*. Company may terminate the Agreement, effective immediately upon notice to Producer, if Producer has violated the terms of this Amendment.