BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is by and between North Shore-LIJ CareConnect Insurance Company, Inc. ("Covered Entity") and _____("Business Associate") (hereinafter, the "Parties") and is effective on the effective date of the Agent/Agency Agreement between the Parties (hereinafter the "Services Agreement"). Unless earlier terminated as provided herein, this Agreement will remain in effect throughout the entire term of the Service Agreement between the Parties.

WHEREAS, Covered Entity and Business Associate have entered into a Services Agreement under which Business Associate will be providing certain services to Covered Entity with respect to the solicitation and sale of Covered Entity's insurance plans;

WHEREAS, in connection with providing services under the Services Agreement, Business Associate will receive, use, disclose, create, maintain and/or Protected Health Information on behalf of Covered Entity; and

WHEREAS, Covered Entity and Business Associate wish to enter into this Agreement governing Business Associate's use and disclosure of Protected Health Information for the purpose of complying with the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended, and implementing privacy and security regulations set forth at 45 C.F.R. Parts 160 through 164, as amended (the "Regulations"), as well as the Health Information Technology for Economic and Clinical Health Act of 2009 and the implementing regulations thereunder, both as amended ("HITECH"), and relevant state law.

NOW, THEREFORE, in consideration of the foregoing recitals and the mutual promises herein made, the Parties agree as follows:

1. Definitions. Any capitalized terms used in this Agreement not otherwise defined herein shall have the meanings ascribed to them in the Regulations or in HITECH.

2. Permitted Uses and Disclosures by Business Associate. Business Associate may use or disclose Protected Health Information only for the following purposes:

2.1 Business Associate may use or disclose Protected Health Information to carry out its obligations under the Services Agreement.

2.2 Business Associate may, to the extent permitted under state and federal law, use or disclose Protected Health Information, if necessary, for Business Associate's proper management and administration or to fulfill any present or future legal responsibilities of Business Associate; provided, however, that if Business Associate discloses Protected Health Information to a third Party for such purpose, Business Associate shall: (i) obtain reasonable assurances from the person to whom the Protected Health Information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was

disclosed to such person and (ii) obligate such person to notify Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.3 Business Associate may use or disclose Protected Health Information as Required By Law.

3. Limitations on Use and Disclosure. Business Associate shall not use or disclose Protected Health Information, except as permitted by Section 2 hereof. Business Associate shall not use or disclose Protected Health Information received from or created on behalf of Covered Entity in a manner that would violate the Regulations (including the minimum necessary requirements thereof) if done by Covered Entity. Business Associate acknowledges and agrees that the requirements of HITECH that relate to privacy or security are applicable to Business Associate in the same manner that such requirements are applicable to Covered Entity. All such requirements are incorporated by reference into this Agreement.

4. Appropriate Safeguards.

4.1 Data Protections. Business Associate shall use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Covered Entity, as required by 45 C.F.R. Parts 160, 162 and 164, as amended by HITECH (the "Security Rule"). Without limiting the generality of the foregoing, Business Associate shall comply with the security standards set forth in 45 C.F.R. Sections 164.308, 164.310, 164.312 and 164.316. Business Associate shall comply with any applicable state data security laws and regulations. In furtherance of compliance with such requirements, Business Associate shall:

4.1.1 maintain an information security program that meets or exceeds the level required by the HIPAA Security Rule and provides for the conducting of risk assessments;

4.1.2 maintain policies and procedures for Business Associate's organization, consistent with the 45 C.F.R Parts 160 and 164, subparts A and E, as amended by HITECH (the "Privacy Rule") and Security Rules;

4.1.3 identify an individual within the Business Associate's organization who is responsible for enforcement and oversight of such privacy and security policies and procedures;

4.1.4 ensure that any and all employees of Business Associate that handle or access Protected Health Information undergo ongoing training regarding the safeguarding of Protected Health Information;

4.1.5 ensure that any and all third parties that access Covered Entity's

confidential data or Protected Health Information with whom Business Associate contracts with or relies upon for the provision of services also maintain a framework for compliance with the Privacy Rule and the Security Rule;

4.1.6 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 Protected Health Information;

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

4.1.8 maintain policies and procedures that specifically address how security Breaches that are identified will be addressed;

4.1.9 maintain technology policies and procedures that provide reasonable safeguards for the protection of Protected Health Information on hardware and software utilized by Business Associate;

4.1.10 comply with all applicable state data security laws and regulations;

4.1.11 to the extent that Business Associate stores, processes and/or transmits cardholder data (e.g, credit card numbers and other related information, as such term is defined by the Payment Card Industry, (PCI) data security standards), Business Associate shall comply with all PCI data security standards;

4.1.12 not transmit, use or disclose Protected Health Information in any form via any medium beyond the boundaries and jurisdiction of the United States without express written authorization from Covered Entity; and

4.1.13 not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual that is disclosed, provided, or made available to Business Associate from Covered Entity.

4.2 Securing Protected Health Information. Business Associate agrees to secure all Protected Health Information, i.e., render all Protected Health Information unusable, unreadable, or indecipherable, consistent with applicable laws and industry guidance, including but not limited to the U.S. Department of Health and Human Services ("HHS") Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements, maintained or held by Business Associate in any format or medium. Such requirements without limitation apply to any and all Protected Health Information (i) in the process of transmission, (ii) residing on computers, servers, portable and non-portable devices and the requirement to encrypt any and all communications that include Electronic Protected Health Information, such as electronic mail, or (iii) that is stored on any Business Associate storage, archival or backup medium. In the event Business Associate hosts or stores any of Covered Entity’s Electronic PHI on storage, archival, or backup medium, Business Associate represents and warrants that it has the capability to support,

and shall at all times and at no charge to Covered Entity use best practices in the healthcare software industry to support, Covered Entity's encryption of all such stored electronic PHI ("ePHI")to ensure the confidentiality, privacy and security of all such ePHI. Business Associate shall ensure that all maintenance, storage and hosting of Covered Entity's data occurs within the United States unless Business Associate obtains Covered Entity's prior written approval. Business Associate agrees that in no event may Protected Health Information and/or Electronic Protected Health Information be stored on any Business Associate portable hardware, including laptops, mobile devices and the like, unless such Protected Health Information is secured and encrypted consistent with the terms of this Agreement. Business Associate further agrees that any and all media on which Protected Health Information is stored or recorded will be destroyed, including but not limited to assuring that hard copy Protected Health Information will be shredded and electronic media will be cleared, purged, or destroyed consistent with National Institute of Standards and Technology Guidelines for Media Sanitization.

4.3 Security Survey. During the term of this Agreement, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Covered Entity 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 a reasonable timeframe specified by Covered Entity shall constitute a material breach of this Agreement.

5. Disclosure to Agents. In the event Business Associate discloses to any agent, including a subcontractor, Protected Health Information received from, or created, received, transmitted or maintained by Business Associate on behalf of Covered Entity, Business Associate shall, in accordance with 45 C.F.R. § 164.502(e)(1)(i)and § 164.308(b)(2), obtain from each such agent or subcontractor an agreement in writing to be bound by the same restrictions, conditions and requirements regarding the use, disclosure and safeguarding of Protected Health Information as are applicable to Business Associate under this Agreement. To the fullest extent permitted by law, Business Associate shall be liable to Covered Entity for any acts, failures or omissions of subcontractors and agents under the Agreement and this Agreement as if such acts, failures or omissions were Business Associate's own acts, failures or omissions.

6. Reporting and Mitigation of Improper Disclosures. Business Associate shall immediately report to Covered Entity any use or disclosure of Protected Health Information not provided for by, or that is in violation of, this Agreement of which Business Associate becomes aware, including Breaches of Unsecured Protected Health Information as required in 45 C.F.R. § 164.410, and any Security Incident of which it becomes aware. Business Associate shall fully cooperate with Covered Entity and make best efforts to mitigate, to the extent practicable, any harmful effects of any improper use or disclosure of Protected Health Information of which it becomes aware. The Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined herein) for which no additional notice to Covered Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's' firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Covered Entity's Electronic PHI.

7. Notification of Breach.

7.1 Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach of individually identifiable information (including but not limited to Protected Health Information, and referred to herein as "Individually Identifiable Information") that if misused, disclosed, lost or stolen could trigger an obligation under state breach notification laws or HITECH.

7.2 Business Associate shall notify Covered Entity of any Breach involving Covered Entity's Unsecured Protected Health Information as set forth herein as soon as reasonably possible after Business Associate's discovery of the Breach, but in no event more than two (2) business days following discovery thereof. For this purpose, discovery means the first day on which the Breach is known to Business Associate, or its subcontractors or agents, or by exercising reasonable diligence would have been known to Business Associate, or its subcontractors or agents. Business Associate shall be deemed to have knowledge of a Breach if the Breach is known or by exercising reasonable diligence would have been known to any person, other than the person committing the Breach, who is an employee, officer, subcontractor or other agent of Business Associate. The notification will include, to the extent known, the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed as a result of such incident, and any other available information in Business Associate's possession which Covered Entity is required to include in the individual notice contemplated by 45 C.F.R. § 164.404. Such report shall include, without limitation, a brief explanation of the event, a description of the types of Protected Health Information involved, a brief description of what Business Associate is doing to investigate the Breach, to mitigate the harm, and to protect against future Breaches; and any other information that Covered Entity reasonably deems necessary to meet its Breach notification obligations under HITECH (or, as applicable, State law).

7.3 Following the Breach, Business Associate will have a continuing duty to supplement its initial notice by informing Covered Entity of new information learned by Business Associate regarding the Breach, including but not limited to the information required to be included in the individual notice. Business Associate shall provide full cooperation to Covered Entity in connection with the investigation of the Breach and notification of affected individuals.

7.4 In addition to the other requirements in this Section 7, Business Associate agrees to implement reasonable systems for the prompt reporting of any breach of Individually Identifiable Information that would trigger an obligation under one or more State data breach notification laws (each a "State Breach") to notify the individuals who are the subject of the information. Business Associate agrees that in the event of a State Breach, Business Associate shall (i) notify Covered Entity within two (2) business days of such State Breach of the nature and scope of the incident giving rise to the State Breach and the individuals impacted; (ii) cooperate and assist Covered Entity with any investigation into any State Breach or alleged State Breach; (iii) take steps to mitigate to the extent practicable any potential harm to individuals impacted by the State Breach; (iv) cooperate and assist Covered Entity with any investigation into any State Breach or alleged State Breach conducted by any State Attorney General or State Consumer Affairs Department (or other similar agency, however so named) (or their respective agents); and (v) assist with any decision by Covered

Entity or State agency to notify individuals impacted or potentially impacted by such State Breach.

7.5 Without limiting Covered Entity's remedies under Section 13 or any other provision of this Agreement, in the event of a Breach involving Unsecured Protected Health Information created, received, maintained, transmitted, used or disclosed by Business Associate or its agents and subcontractors, Business Associate shall reimburse Covered Entity for the cost of production and delivery of any legally required notice to affected Individuals and the cost of credit monitoring for such Individuals to the extent deemed reasonably necessary by Covered Entity. In addition, Business Associate shall reimburse Covered Entity for any expense Covered Entity determines to be necessary to mitigate any Breach or State Breach or harmful effect of any Security Incident related to Protected Health Information that is caused by Business Associate's negligence or deliberate act or any other non-permitted use or disclosure of Protected Health Information by Business Associate, which expenses may include, but not be limited to investigation costs and expenses, employee wages and salaries, delivery services, printing, postage, telephone costs, website design, advertising expenses, attorneys' fees, credit monitoring costs, all individual, media, and government notification costs and expenses, and any other expenses or costs related to Breach, State Breach, Security Incident or other non-permitted use or disclosure of Protected Health Information.

8. Individual Rights.

8.1 Upon request, and in the time and manner designated by Covered Entity, Business Associate shall provide to Covered Entity (or, as directed in writing by Covered Entity, to an Individual or the Individual's designee) all Protected Health Information in Business Associate's possession necessary for Covered Entity to provide Individuals or their representatives with access to or copies thereof in accordance with the Regulations and HITECH. If Business Associate receives a request directly from an Individual or the Individual's designee, Business Associate shall notify Covered Entity as soon as administratively feasible, but in no event later than three (3) business days, in order for the Parties to coordinate a response.

8.2 Upon request, and in the time and manner designated by Covered Entity, Business Associate shall provide to Covered Entity all information and records in Business Associate's possession necessary for Covered Entity to provide Individuals or their representatives with an accounting of disclosures thereof in accordance with the Regulations and HITECH. Business Associate shall track and record all such disclosures to ensure compliance with this section.

8.3 Upon request, and in the time and manner designated by Covered Entity, Business Associate shall provide to Covered Entity all Protected Health Information in Business Associate's possession necessary for Covered Entity to respond to a request by an Individual to amend such Protected Health Information in accordance with the Regulations. In the event that Covered Entity amends any Protected Health Information in its possession, a copy of which is also retained by Business Associate, Covered Entity shall promptly notify Business Associate of such amendment. At Covered Entity's direction, Business Associate shall promptly incorporate any amendments to Protected Health Information made by Covered Entity into the information maintained by Business Associate.

8.4 Business Associate shall promptly comply with any restrictions on the uses of Protected

Health Information agreed to by Covered Entity in accordance with the Regulations immediately upon written notification by Covered Entity.

9. Access by HHS and Covered Entity. Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available, without charge, to HHS or Covered Entity to enable HHS or Covered Entity to evaluate Business Associate's compliance with the Regulations and HITECH. Except to the extent prohibited by law, Business Associate agrees to notify Covered Entity immediately upon receipt by Business Associate of any and all requests by or on behalf of any and all federal, state and local authorities served upon Business Associate for Protected Health Information.

10. De-identification and Limited Data Sets. Covered Entity retains all rights in the Protected Health Information. Except to provide Services to Covered Entity, Business Associate shall not de-identify Protected Health Information without the express written permission of Covered Entity. In no event shall Business Associate create a Limited Data Set from Protected Health Information received from or created on behalf of Covered Entity without express written permission of Covered Entity.

11. Return of Protected Health Information. Upon termination of this Agreement, Business Associate shall, if feasible, return or destroy (as directed by Covered Entity) all Protected Health Information received from, or created or received by Business Associate or any of its agents or subcontractors on behalf of, Covered Entity that Business Associate or any of its agents and subcontractors still maintains in any form, and Business Associate and its agents and subcontractors shall retain no copies of such information. If such return or destruction is not feasible (e.g., due to state law obligations to retain such Protected Health Information), Business Associate shall provide notice to Covered Entity of the conditions that make such return or destruction infeasible. Upon mutual agreement by the Parties that such return or destruction is infeasible, Business Associate shall extend all of the protections of this Agreement to such information and limit further uses and disclosures to those purposes that make the return or destruction of the Protected Health Information infeasible, despite termination of this Agreement. For the avoidance of doubt, this provision shall expressly apply to Protected Health Information that is in the possession of agents or subcontractors of Business Associate.

11.1 Both Parties represent that in exchanging electronic data, they will comply with applicable HIPAA and HITECH regulations concerning security and standard and electronic transactions, and specifically, neither Party will: (i) change the definition, data condition, or use of a data element or segment in a standard transaction; (ii) add any data elements or segments to the maximum defined data set; (iii) use any code or data elements that are either marked "not used" in the standard's implementation specification(s) or are not in the standard's implementation specification(s); or (iv) change the meaning or intent of the standard's implementation specifications.

12. Obligations of Covered Entity.

12.1 Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices issued by Covered Entity pursuant to 45 C.F.R. § 164.520 to the extent that such

limitation may affect Business Associate's use or disclosure of Protected Health Information.

12.2 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

12.3 Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information to the extent that such changes may affect Business Associate's use or disclosure of such information.

13. Indemnification. Notwithstanding anything in the Services Agreement to the contrary, Business Associate shall indemnify, defend and hold harmless Covered Entity and its affiliates and their respective officers, directors, employees and agents from and against any claims, losses, expenses or other costs (including, but not limited to, reasonable attorneys' fees, compliance with applicable notice provisions and credit monitoring services, administrative fines and penalties assessed by the Secretary of HHS or other regulatory authority, and any award that may be made pursuant to a State Attorney General action) arising from or relating to: (i) the breach of this Agreement by Business Associate or (ii) any use or disclosure of Individually Identifiable or Protected Health Information by Business Associates or its employees or agents or subcontractors that does not comply with the terms of this Agreement. This Section 13 shall not be subject to any limitations of liability set forth in the Services Agreement.

14. State Law. Business Associate agrees to comply with obligations of applicable State and federal laws and/or regulations with respect to personal information, including but not limited to the confidentiality, disclosure and re-disclosure requirements of 10 NYCRR Part 63 and the breach notification requirements in the New York State Information Security Breach and Notification Act (General Business Law Section 899-11, State Technology Law Section 208), and Business Associate agrees to ensure that any agent or subcontractor complies with all such requirements. Business Associate agrees to provide training to its employees and any other Workforce members who have access to protected information under state law, and to ensure that its agents and subcontractors do the same.

15. Term and Termination.

15.1 The term of this Agreement shall be from the effective date of the Services Agreement until termination or expiration of the Services Agreement.

15.2 Notwithstanding any other provision of this Agreement, Covered Entity is authorized to immediately terminate this Agreement if Covered Entity determines that Business Associate has violated a material term of this Agreement. Upon termination of this Agreement, the Services Agreement shall automatically terminate simultaneously therewith.

15.3 In the event either Party becomes aware that the other Party has engaged in a pattern of activity or practice that constitutes a material breach or violation of the terms of this Agreement, the non-breaching Party may request in writing that the breaching Party cure the breach or

violation. If the breach or violation is not cured within a reasonable time period specified by the non-breaching Party, the non-breaching Party may terminate this Agreement and the Services Agreement; provided, however, if termination is not feasible, the non-breaching Party shall report the breach or violation to the Secretary of HHS.

16. Miscellaneous.

16.1 Amendment. If HIPAA, the Regulations or HITECH are amended or interpreted in any manner that Covered Entity reasonably believes renders this Agreement inconsistent therewith, Covered Entity may in its discretion, amend this Agreement to comply with such amendments or interpretations by providing thirty (30) days advance written notice to Business Associate (or any shorter notice period necessary to comply with such amendment or interpretation). Such Amendment will become effective if Business Associate does not object during that thirty (30) day notice period.

16.2 Survival. Termination or expiration of this Agreement shall not terminate any provision of this Agreement which by its terms is to survive or be performed following termination or expiration, unless otherwise expressly agreed in writing by the Parties. Termination or expiration of this Agreement shall not affect or impair any rights or obligations arising prior to or at the time of termination or expiration. Following termination or expiration of this Agreement, each Party shall remain liable for any obligations or liabilities arising from its performance (or failure to perform) its obligations under this Agreement prior to such termination or expiration. For the avoidance of doubt, Business Associate's obligations, and Covered Entity's rights, under Sections 6, 7, 8, 9, 10, 11, 13 and 14 shall survive the termination or expiration of this Agreement for any reason.

16.3 Full Authority. Each Party hereto represents and warrants to the other Party that it has the legal power and authority to enter into and perform its obligations under this Agreement without violating the rights or obtaining the consent of any third Party.

16.4 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA and HITECH.

16.5 Miscellaneous. Except as otherwise set forth in this Section 16.5 of this Agreement, in the event of a conflict between the terms of this Agreement and the terms of the Services Agreement, the terms of this Agreement shall prevail. The terms of the Services Agreement which are not modified by this Agreement shall remain in full force and effect in accordance with the terms thereof. The Services Agreement together with this Agreement constitutes the entire agreement between the Parties with respect to the subject matter contained herein. This Agreement may be executed by fax, and/or in any number of counterparts, all of which shall together be considered an original and may be evidenced by a fax or scanned electronic (e.g. .pdf, .tif) copy.

[SIGNATURES TO FOLLOW ON NEXT PAGE]

IN WITNESS WHEREOF, each party hereby executes this Agreement by its duly authorized representative.

NORTH SHORE-LIJ CARECONNECT INSURANCE COMPANY, INC.
By:
Name & Title:
Date:

By:
Name & Title:
Date:

82938011\V-7