Sun Life Financial

Producer Business Associate Policy

Pursuant to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations at 45 C.F.R Parts 160-164 (collectively "HIPAA") Sun Life Assurance Company of Canada, Sun Life and Health Insurance Company (U.S.) and certain other affiliates (collectively "the Company") and Business Associates are required to regulate the use and disclosure of certain individually identifiable information. Insurance producers and other distributors contracted with or appointed by the Company to sell products subject to HIPAA who are provided PHI by on behalf of the Company for the purpose of selling or administering insurance coverage qualify as Business Associates and are required to comply with the provisions of this Producer Business Associate Policy ("Policy").

This Policy is limited to the extent that the Company is a Covered Entity as defined below. This Policy constitutes a Company policy, rule, guideline, or any other form of statement which creates an obligation under applicable producer agreements or conditions of employment. Unless otherwise stated, this Policy shall apply to all services between the Business Associate and Sun Life.

The Business Associate has access to Protected Health Information ("PHI"), through its services in providing licensed insurance sales and brokerage.

HIPAA requires written agreements or arrangements with business associates to regulate the use and disclosure of Protected Health Information; Business Associates also have independent compliance obligations under the Privacy Standards and Security Standards.

In order to disclose and protect information given to the Business Associate, some of which may constitute PHI, the Business Associate and Sun Life agree to the following:

1. Definitions. All terms that are used but not otherwise defined in this Policy shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance. In addition to the terms in the Agreement, the following terms when capitalized will have this meaning:

a. Breach. "Breach" shall have the same meaning as the term "Breach" in 45 CFR § 164.402.

b. Business Associate. "Business Associate" shall have the meaning provided for in 45 CFR 160.103.

c. Covered Entity. "Covered Entity" shall mean Sun Life Assurance Company of Canada, and Sun Life and Health Insurance Company (U.S.).

d. Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR § 164.501.

e. Electronic Health Record. "Electronic Health Record" shall have the same meaning as the term "electronic protected health information" in American Recovery and Reinvestment Act of 2009,§ 13400(5).

f. Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103.

g. Electronic Transactions Rule. "Electronic Transactions Rule" shall mean the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.

h. HHS. "HHS" shall mean the Department of Health and Human Services.

i. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, subparts A and E.

j. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

k. Required By Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR § 160.103.

l. Security Incident. "Security Incident" shall have the same meaning as the term "securing incident" in 45 CFR § 160.103.

m. Security Rule. "Security Rule" shall mean the Security Standards and Implementation Specifications at 45 CFR Parts 160 and 164, subpart C.

n. Transaction. 'Transaction" shall have the meaning given the term "transaction" in 45 CFR § 160.103.

o. Unsecured Protected Health Information. "Unsecured protected health information" shall have the meaning given the term "unsecured protected health information" in 45 CFR § 164.402.

2. Business Associate's Operations. Business Associate of Sun Life, agrees to comply with all applicable privacy and security laws and regulations, including those set forth in the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. 142, 160, 162 and 164) ("HIPAA"), as may be amended from time to time, and any other applicable Privacy and Security Law as a Business Associate of Sun Life.

3. Safeguarding Privacy and Security of Protected Health Information

a. Permitted Uses and Disclosures. Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on Covered Entity's behalf or receives from Covered Entity (or another business associate of Covered Entity) and to request Protected Health Information on Covered Entity's behalf (collectively, "Covered Entity's Protected Health Information") only:

i. Functions and Activities on Covered Entity's Behalf. To act as the agent of record for group insurance plans.

ii. Business Associate's Operations. For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that, with respect to disclosure of Covered Entity's Protected Health Information, either:

1. The disclosure is Required by Law; or

2. Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Covered Entity's Protected Health Information that the person or entity will: (1) Hold Covered Entity's Protected Health Information in confidence and use or further disclose Covered Entity's Protected Health Information only for the purpose for which Business Associate disclosed Covered Entity's Protected Health Information to the person or entity or as Required by Law; and (2) Promptly notify Business Associate (who will in turn notify Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of Covered Entity's Protected Health Information was breached.

3. Minimum Necessary. Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of Covered Entity's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, consistent with this Policy and the Privacy Rule, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither Business Associate nor Covered Entity is required to limit its use, disclosure or request to the minimum necessary. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), passed as part of the American Recovery and Reinvestment Act of 2009, and government guidance on the definition.

b. Prohibition on Unauthorized Use or Disclosure. Business Associate will neither use nor disclose Covered Entity's Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Covered Entity's Protected Health Information in a manner that will violate the Privacy Rule if done by Covered Entity.

c. Information Safeguards. Business Associate will provide the following Information Safeguards:

i. Privacy of Covered Entity's Protected Health Information. Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards (“Safeguards”) to protect the privacy of Covered Entity's Protected Health Information. Safeguards must reasonably protect Covered Entity's Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit

incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement.

ii. Security of Covered Entity's Electronic Protected Health Information. Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of, and to prevent non-permitted or violating use or disclosure of, electronic Protected Health Information created, transmitted, maintained or received in connection with the services, functions, and/or transactions to be provided under this Policy or the Service Agreement, consistent with the requirements of the HIPAA Security Rule, and will comply with all requirements of such Security Rule. Business Associate will document and keep these Safeguards current. Business Associate agrees to provide training to its workforce as required by 45 CFR 164.530. Business Associate will comply with any additional requirements as requested by Covered Entity.

d. Subcontractors and Agents. Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted by this Policy or in writing by Covered Entity to disclose Covered Entity's Protected Health Information *and/or* Electronic Protected Health Information, to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to Covered Entity's Protected Health Information and/or Electronic Protected Health Information that are applicable to Business Associate under this Policy.

e. Prohibition on Sale of Records. As of the effective date specified by HHS in final regulations to be issued on this topic, Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtained from the individual, in accordance with 45 CFR § 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under the HITECH Act.

f. Penalties for Non-compliance. Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the privacy rule and security rule, as amended by the HITECH Act.

4. Compliance with Electronic Transactions Rule. If Business Associate conducts in whole or part electronic Transactions on behalf of Covered Entity for which HHS has established standards, Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule. Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

5. Individual Rights. Business Associate will maintain the following rights for individuals:

a. Access. Business Associate will, within twenty (20) calendar days following Covered Entity's request, make available, in a time and manner required by the Privacy Rule, and in a Designated Record Set where permitted and appropriate, Covered Entity's Protected Health Information

about the individual that is in Business Associate's custody or control to Covered Entity or, at Covered Entity's direction, to an individual (or the individual's personal representative) for inspection and obtaining copies so that Covered Entity may meet its access obligations under 45 CFR § 164.524. Effective as of the date specified by HHS, if the Protected Health Information is held in an Electronic Health Record, then the individual shall have a right to obtain from Business Associate a copy of such information in an electronic format. Business Associate shall provide such a copy to Covered Entity or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously, and specifically made by the individual or Covered Entity.

b. Amendment. Business Associate will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of Covered Entity's Protected Health Information, so that Covered Entity may meet its amendment obligations under 45 CFR § 164.526.

c. Disclosure Accounting. Business Associate will facilitate Covered Entity's ability to meet its disclosure accounting obligations under 45 CFR § 164.528 in the following manner:

i. Disclosures Subject to Accounting. Business Associate will record the information specified below ("Disclosure Information") for each disclosure of Covered Entity's Protected Health Information, not excepted from disclosure accounting as specified below, that Business Associate makes to Covered Entity or to a third party.

ii. Disclosures Not Subject to Accounting. Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Covered Entity's Protected Health Information if Covered Entity need not account for such disclosures.

iii. Disclosure Information. With respect to any disclosure by Business Associate of Covered Entity's Protected Health Information that is not excepted from disclosure accounting, Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

1. Disclosure Information Generally. Except for repetitive disclosures of Covered Entity's Protected Health Information as specified below, the Disclosure Information that Business Associate must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a brief description of Covered Entity's Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.

2. Disclosure Information for Repetitive Disclosures. For repetitive disclosures of Covered Entity's Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including Covered Entity), the Disclosure Information that Business Associate must record is either the Disclosure Information specified above for each accountable disclosure, or (i) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (ii) the frequency, periodicity, or number of the repetitive accountable disclosures; and (iii)

the date of the last of the repetitive accountable disclosures (iv) Availability of Disclosure Information. Business Associate will maintain the Disclosure Information for at least six (6) years following the date of the accountable disclosure to which the Disclosure Information relates (Three (3) years for disclosures related to an Electronic Health Record, starting with the date specified by HHS). Business Associate will make the Disclosure Information available to Covered Entity within twenty (20) calendar days following Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. Effective as of the date specified by HHS, with respect to disclosures related to an Electronic Health Record, Business Associate shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual.

d. Restriction Agreements and Confidential Communications. Business Associate will comply with any agreement that Covered Entity makes that either (i) restricts use or disclosure of Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(a), or (ii) requires confidential communication about Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(b), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement. Effective February 17, 2010 (or such other date specified as the effective date by HHS), Business Associate will comply with any restriction request if (i) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

6. Breaches and Security Incidents. Breaches and Security Incidents shall be handled in the following manner:

a. Reporting. Business Associate will report Breaches, suspected Breaches and Security Incidents as follows:

i. Privacy or Security Breach. Business Associate will report promptly to Covered Entity any use or disclosure of Covered Entity's Protected Health Information not provided for by this Agreement along with any Breach or suspected Breach of Covered Entity's Unsecured Protected Health Information. Business Associate will treat the Breach as being discovered in accordance with 45 CFR § 164.410. Business Associate also shall notify Covered Entity within ten days of any Breach of "Undisclosed Protected Health Information" as defined by the Breach Notification Rule set forth at 45 CFR Part 164 Subpart D. Any such report shall include the identification (if known) of each individual whose Unsecured Protected Healthy Information has been, or is reasonably believed by Business Associate to have been,

accessed, acquired, or disclosed during such Breach. Further, Business Associate's notification shall at least:

- Identify the nature of the non-permitted use or disclosure or other breach;
- Identify the PHI used, accessed or disclosed;
- Identify who made the non-permitted use or received the non-permitted disclosure;
- Identify what corrective action Business Associate took or will take to prevent further non-permitted uses or disclosures;
- Identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and
- Provide such other information, including a written report, as Covered Entity may reasonably request.

ii. Security Incidents. Business Associate will report to Covered Entity any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's Electronic Protected Health Information or (B) interference with Business Associate's system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate will make this report upon request, except if any such security incident resulted in a disclosure not permitted by this Agreement or Breach of Covered Entity's Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth in the paragraph above.

7. Term and Termination.

a. Term. The term of this Policy shall terminate when all Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

b. Right to Terminate for Cause. Covered Entity may terminate Policy if it determines, in its sole discretion, that Business Associate has breached any provision of this Policy, and upon written notice to Business Associate of the breach, Business Associate fails to cure the breach within thirty (30) calendar days after receipt of the notice. *Any* such termination will be effective immediately or at such other date specified in Covered Entity's notice of termination.

c. Return or Destruction of Covered Entity's Protected Health Information as Feasible. Upon termination or other conclusion of this Policy, Business Associate will, if feasible, return to Covered Entity or destroy all of Covered Entity's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Covered Entity's Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Business Associate. Further, Business Associate shall require any such subcontractor or agent to certify to Business Associate that it returned to Business Associate (so that Business Associate may return it to the Covered Entity) or destroyed all such information which could be returned or destroyed. Business Associate will

complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Policy.

d. Procedure When Return or Destruction Is Not Feasible. Business Associate will identify any of Covered Entity's Protected Health Information, including any that Business Associate has disclosed to subcontractors or agents as permitted under this Policy, that cannot feasibly be returned to Covered Entity or destroyed and explain why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of Policy.

e. Continuing Privacy and Security Obligation. Business Associate's obligation to protect the privacy and safeguard the security of Covered Entity's Protected Health Information as specified in this Policy will be continuous and survive termination or other conclusion of this Policy, or the underlying Agreement.

8. General Provisions.

a. Inspection of Internal Practices, Books, and Records. Business Associate will make its internal practices, books, and records relating to its use and disclosure of Covered Entity's Protected Health Information, and its policies and procedures and related documentation pursuant to the Security Rule, available to Covered Entity and to HHS to determine compliance with the Privacy Rule and Security Rule.

b. Amendment to Policy. Upon the compliance date of any final regulation or amendment to final regulation promulgated by HHS that affects Business Associate or Covered Entity's obligations under this Policy, this Policy will automatically amend such that the obligations imposed on Business Associate or Covered Entity remain in compliance with the final regulation or amendment to final regulation.

c. No Third-Party Beneficiaries. Nothing in this Policy shall be construed as creating any rights or benefits to any third parties.

d. Interpretation. Any ambiguity in the Policy shall be resolved to permit Covered Entity and Business Associate to comply with the applicable requirements under HIPAA.

e. Indemnification. *[Add if there is nothing specific in the underlying agreement]* The Parties agree to indemnify each other and each respective director, officer, employee and agent, from and against all actions, liabilities damages, injuries, judgments and external expenses including all incidental expenses in connection with such liabilities, obligations, claims or actions based upon or arising out of damages sustained in connection with the performance of this Policy, brought, alleged or incurred and based upon:

i. Any alleged or actual violation of any law or regulation by either Party or any of its Affiliates or representatives; or

ii. The gross negligence or willful misconduct of either Party or any of its Affiliates or representatives; or

iii. The improper or illegal use or disclosure of, whether negligent or willful, of any PHI.

f. Subpoenas. Business Associate agrees to provide notice to Covered Entity of any subpoena or other legal process seeking PHI received from or created on behalf of Covered Entity or its affiliates. Such notice shall be provided within forty-eight (48) hours of receipt.

g. State Law. Where the mandatory terms of the HIPAA Privacy or Security Rule conflict with obligations imposed under state law, the Federal law shall govern.

h. Assignment. Upon written notice to Business Associate, Covered Entity shall have the right to assign this Policy to any successor or affiliate company. Business Associate may not assign this Policy without prior written consent, which will not be unreasonably withheld.

i. Paragraph Headings. Paragraph headings are for reference purposes only and shall not affect in any way the meaning or interpretation of this Policy.

j. Recitals. The recitals contained in the preamble to this Policy are made a part of the terms, provisions and conditions, and shall be binding on the parties as if fully set forth within the Policy.