



MEDICAL PROFESSIONAL MUTUAL INSURANCE COMPANY

MHA INSURANCE COMPANY

PROSELECT INSURANCE COMPANY

WASHINGTON CASUALTY COMPANY

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT BUSINESS ASSOCIATE TERMS AND CONDITIONS

WHEREAS, the Standards for Privacy and Security of Individually Identifiable Health Information regulation promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-1329d-8; 42 U.S.C. 1320d-2) and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, (collectively, "HIPAA") establishes federal requirements for the use, disclosure, and security of individually identifiable health information;

WHEREAS, HIPAA's implementing regulations require health care providers to enter into written agreements or other arrangements with business associate(s) that govern the business associate's use and/or disclosure of individually identifiable health information;

WHEREAS, the Insured, a health care provider, is seeking, or has obtained, insurance coverage from one of the companies identified above (the "Company");

WHEREAS, many states have implemented laws that establish certain requirements governing the protection of personal information of state residents ("Personal Information"), some of which may be applicable to the Company;<sup>1</sup>

WHEREAS, in connection with the Insured obtaining or maintaining such insurance coverage, or in connection with the Insured obtaining benefits under such insurance coverage, the Insured may disclose Protected Health Information, including Electronic PHI (each as defined herein), and/or Personal Information to the Company;

WHEREAS, pursuant to HIPAA, the Company's receipt, use, and redisclosure of such Protected Health Information, including Electronic PHI, in connection with providing such insurance coverage and services related thereto is considered a business associate function of the Insured; and

WHEREAS, the Company desires to enter into or amend and restate, as the case may be, a business associate agreement (this "Agreement") in favor of the Insured on the terms and

---

<sup>1</sup> For example, Massachusetts has laws and regulations governing the protection of Personal Information of its residents (*See M.G.L. c. 93H et seq; 201 CMR 17.00 et seq*). Massachusetts defines Personal Information as a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

conditions set forth herein, pursuant to 45 CFR 164.504(e), to govern the Company's use and disclosure of Protected Health Information, including Electronic PHI, received directly from, or received on behalf of, the Insured.

NOW THEREFORE, in consideration of the mutual promises and covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Company hereto agrees as follows:

1. **Definitions.** Capitalized terms used in this Agreement that are not defined in this Section 1 or elsewhere in this Agreement shall have the respective meanings assigned to such terms in the administrative simplification section of HIPAA and its implementing regulations. The following terms shall have the meanings ascribed thereto for purposes of this Agreement:

**“Electronic Media”** means the mode of electronic transmissions, and includes the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

**“Electronic PHI”** means Protected Health Information which is transmitted by Electronic Media or maintained in Electronic Media.

**“Insured”** means the first named insured and any other insureds as defined under the coverage provided by the Company or the first applicant listed on the application and any other applicants seeking coverage under the same application, provided however, that neither this definition nor this agreement should be construed as an offer of coverage.

**“Privacy and Security Standards”** means the privacy and security standards contained in HIPAA and all regulations promulgated thereunder, including all applicable requirements contained in 45 C.F.R. Parts 160 and 164 currently in effect or as amended.

**“Protected Health Information”** means information that:

- (i) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and (a) identifies the individual, or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- (ii) the Company (a) has received from the Insured, or (b) has received on behalf of the Insured.

**“Representatives”** means with respect to the Company or the Insured, as the case may be, its affiliates, managers, trustees, directors, officers, controlling persons, members, shareholders, employees, producers (including brokers and agents), advisors (including but not limited to accountants, attorneys and financial advisors) and other representatives.

**“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**“Services”** include, without limitation, the business management and general administrative activities of the Insured (including the provision of professional liability insurance coverage, placing stop-loss and excess of loss or re-insurance, receiving and evaluating incidents, claims, and lawsuits relating to such insurance coverage, and providing data analyses for the Insured); conducting quality assessment and quality improvement activities, including outcomes evaluation and the development of clinical guidelines and loss prevention tools; reviewing the competence or qualifications of the Insured’s health care professionals; evaluating the Insured’s practitioner and provider performance; conducting training programs to improve the skills of the Insured’s health care practitioners and providers; conducting credentialing activities; conducting or arranging for medical review; arranging for legal services; and resolution of internal grievances.

2. **HIPAA Amendments.** The Company acknowledges and agrees that the Health Information Technology for Economic and Clinical Health Act and its implementing regulations (collectively, “HITECH”) impose new requirements with respect to privacy, security and breach notification and contemplates that such requirements shall be implemented by regulations to be adopted by the Department of Health and Human Services. The HITECH provisions applicable to business associates will be collectively referred to as the “HITECH BA Provisions.” The provisions of HITECH and the HITECH BA Provisions are hereby incorporated by reference into this Agreement as if set forth in this Agreement in their entirety. Notwithstanding anything to the contrary, the HITECH BA Provisions are automatically effective and incorporated herein: (a) with respect to any security breach notification provision, September 23, 2009; and (b) with respect to the other HITECH BA Provisions, February 17, 2010 or such subsequent date as may be specified in HITECH or applicable final regulations.
3. **Obligations of the Company.** The Company shall not use or disclose Protected Health Information other than as permitted in accordance with the terms of this Agreement.
  - (a) **Permitted Purposes for Use and/or Disclosure of Protected Health Information.** The Company may only:
    - (i) use and/or disclose Protected Health Information in providing the Services to the Insured in connection with the Insured obtaining and maintaining any insurance coverage offered by the Company, including the Insured obtaining any benefits under such insurance coverage; provided that, in connection with the Company’s provision of such Services, the Company shall not, and shall ensure that its Representatives do not, use or disclose Protected Health Information received from the Insured or its Representatives in any manner that would constitute a violation of the Privacy and Security Standards if done by the Insured;
    - (ii) use Protected Health Information for the provision of data aggregation services relating to the health care operations of the Insured;

- (iii) use Protected Health Information for the proper management and administration of the Company;
  - (iv) disclose Protected Health Information to a third party for the Company's proper management and administration, provided that the disclosure is required by law or the Company obtains reasonable assurances from the third party to whom the Protected Health Information is to be disclosed that the third party will (a) protect the confidentiality of the Protected Health Information, (b) only use or further disclose the Protected Health Information as required by law or for the purpose for which the Protected Health Information was disclosed to the third party and (c) notify the Company of any instances of which the person is aware in which the confidentiality of the Protected Health Information has been breached;
  - (v) "de-identify" Protected Health Information or create a "limited data set," and to use "de-identified" information in a manner consistent with and permitted by HIPAA;
  - (vi) use Protected Health Information to carry out the legal responsibilities of the Company;
  - (vii) disclose Protected Health Information as required by law;
  - (viii) to the extent required by the "minimum necessary" requirements of HIPAA, request, use and disclose the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, use or disclosure and, to the extent practicable, omit Direct Identifiers from any request, use or disclosure of Protected Health Information consistent with the HIPAA Limited Data Set standard; and
  - (ix) use and/or disclose Protected Health Information as otherwise agreed to in writing by the Insured.
- (b) **Safeguards Against Misuse of Information.** The Company agrees that it will use appropriate safeguards to prevent the use or disclosure of Protected Health Information in a manner contrary to the terms and conditions of this Agreement and will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI that the Company creates, receives, maintains, or transmits on behalf of the Insured.
- (c) **Reporting of Improper Disclosures of PHI.**
- (i) If the Company becomes aware of a use or disclosure of Protected Health Information in violation of this Agreement by the Company or a third party to which the Company disclosed Protected Health Information, the Company shall report the use or disclosure to the Insured without unreasonable delay.
  - (ii) The Company shall report any Security Incident involving Protected Health Information of which it becomes aware in the following manner:

(a) any actual, successful Security Incident will be reported to the Insured in writing without unreasonable delay, and (b) any attempted, unsuccessful Security Incident directly affecting a system that stores Protected Health Information of which the Company becomes aware will be reported to the Insured orally or in writing on a reasonable basis, as requested by the Insured. If the HIPAA security regulations are amended to remove the requirement to report unsuccessful attempts at unauthorized access, the requirement hereunder to report such unsuccessful attempts will no longer apply as of the effective date of the amendment.

(iii) The Company shall: (a) following the discovery of a Breach of Unsecured Protected Health Information, notify the Insured of the breach without unreasonable delay and in no case later than 60 days after discovery of the breach; and (b) following a breach of Personal Information under any applicable state law, provide any required notifications in accordance with such law.

(d) **Agreements by Third Parties.**

(i) Except as otherwise provided herein, with respect to each agent or subcontractor who (a) performs a Service that the Company has agreed to perform for, or on behalf of, the Insured, and (b) has or will have access to Protected Health Information, the Company shall obtain and maintain an agreement pursuant to which such agent or subcontractor shall agree to be bound by the same types of restrictions, terms and conditions that apply to the Company pursuant to this Agreement with respect to such Protected Health Information.

(ii) With respect to any third party to whom the Company discloses Protected Health Information for a purpose described in Section 3(a)(iii) or 3(a)(v) of this Agreement, the Company shall obtain reasonable assurances from such third party that the Protected Health Information will be held confidentially and will be used or further disclosed only as required by law or for the purpose for which the Company disclosed the Protected Health Information to the third party and that it will implement reasonable and appropriate safeguards to protect it. In addition, such third party shall agree to notify the Company of any instances of which it is aware in which the confidentiality of the information has been breached.

(e) **Access to Information.** In the event that the Company receives a written request by the Insured for access to Protected Health Information, the Company shall, in a timely manner in order to permit the Insured to comply with its obligations under HIPAA, make available to the Insured such Protected Health Information. This obligation shall continue only for so long as such information is maintained by the Company. In the event that any individual requests access to Protected Health Information pertaining to such individual directly from the Company, the Company shall forward such request to the Insured. The provision of access to the individual of such Protected Health Information and/or denial of the same (including the creation and/or maintenance of any notifications and/or documents in connection therewith) shall be the sole responsibility of the Insured.

- (f) **Availability of Protected Health Information for Amendment.** In the event that the Company receives a written request from the Insured for the amendment of an individual's Protected Health Information, the Company shall, in a timely manner in order to permit the Insured to comply with its obligations under HIPAA, make available such Protected Health Information to the Insured. This obligation shall continue only for so long as such information is maintained by the Company. In the event that the Insured agrees to comply with an individual's request to amend such Protected Health Information, the Company shall incorporate any such amendments designated by the Insured. In the event that the Insured denies an individual's request to amend such Protected Health Information, the Company shall incorporate into the Protected Health Information any of the statements and/or documents that the Insured has created or received with respect to such denial; provided that, the Insured has provided the Company with a copy of such statement and/or documents. In the event that any individual requests an amendment to Protected Health Information pertaining to such individual directly from the Company, the Company shall forward such request to the Insured. The determination of whether to amend such Protected Health Information pursuant to an individual's request and/or the denial of such request (including the creation and/or maintenance of any notification and/or creation of documents in connection therewith) shall be the sole responsibility of the Insured.
- (g) **Accounting of Disclosures.** The provisions of this Section 3(g) apply solely to those accountings of disclosures of Protected Health Information that are required of a health care provider pursuant to 45 C.F.R. § 164.528. In the event that the Company receives a written request from the Insured for such an accounting, the Company shall provide the following information to the Insured with respect to each disclosure the Company has made: (a) the date of the disclosure, (b) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person, (c) a brief description of the Protected Health Information disclosed, and (d) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. The Company shall provide such information with respect to each disclosure made for the period of time noted in the Insured's request, which shall not exceed six (6) years from the date of Insured's request. If, during the period covered by the accounting, the Company has made multiple disclosures of Protected Health Information either (a) to the same person or entity, or (b) for a particular research purpose, the accounting information provided to the Insured may be modified as described in 45 CFR 164.528(b)(3) or 45 CFR 164.528(b)(4), as applicable. The Company shall provide such accounting to the Insured in a timely manner in order to permit the Insured to comply with its obligations under HIPAA. In the event that the request for an accounting is delivered directly to the Company, the Company shall forward such request to the Insured. The provision of such accounting of such disclosures to the individual (including the creation and/or maintenance of any notifications and/or documents in connection therewith) shall be the sole responsibility of the Insured.
- (h) **Availability of Books and Records.** Except as otherwise prohibited by law, the Company hereby agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information in connection with its obligations under this Agreement available to the Secretary of Health and Human

Services for purposes of determining the Insured's compliance with the Privacy and Security Standards.

- (i) **Use of Limited Data Set.** In the event that the Company receives or creates a limited data set (as defined under HIPAA), then the Company shall only use and disclose such limited data set for research purposes, public health purposes or as otherwise required by law. In addition, the Company shall comply with Section 3(b), Section 3(c), and Section 3(d)(i) of this Agreement in the same manner as though such Sections referenced a limited data set, instead of Protected Health Information. Finally, except as otherwise permitted pursuant to this Agreement, the Company shall not re-identify the limited data set such that the limited data set becomes Protected Health Information and shall not contact any individual who is the subject of the limited data set.
  - (j) **Maintenance of Records.** Subject to Section 7 below, the Company shall maintain all records created pursuant to this Agreement for a period of at least six (6) years from the date of the creation of such records. This Section 3(j) shall survive termination of this Agreement.
4. **Personal Information.** To the extent that the Company has access to Personal Information, the Company agrees that it has implemented and maintains appropriate security measures for the protection of Personal Information in accordance with applicable state laws.
5. **Obligations of the Insured.** The Insured shall have obtained all necessary consents and/or authorizations required under state law to enable the Insured to lawfully disclose the Protected Health Information to the Company and to enable the Company to use and disclose the Protected Health Information in accordance with the terms of this Agreement. In addition, to the extent the Protected Health Information contains any psychotherapy notes (as defined under HIPAA), the Insured agrees to obtain all necessary authorizations to enable the Insured to lawfully disclose the Protected Health Information to the Company and to enable the Company to use and disclose the Protected Health Information in accordance with the terms of this Agreement.
6. **Term and Termination.** This Agreement shall remain in full force and effect until one of the following occurs (each, a "Termination Event"): (a) the Company denies either the Insured's application for insurance coverage or the Insured's application for renewal of insurance coverage; (b) the Company or the Insured terminates the Insured's insurance coverage; (c) the Insured's insurance coverage with the Company expires; or (d) the Insured determines that the Company has breached a material term of this Agreement.
7. **Return or Destruction of Protected Health Information.** After the occurrence of a Termination Event, the Company shall either return or destroy all Protected Health Information, if any, which the Company still maintains. The Company shall not retain any copies of such Protected Health Information. Notwithstanding the foregoing, to the extent that the Company determines it is not feasible to return or destroy such Protected Health Information, the terms and provisions of Section 3 shall survive termination of this Agreement and such Protected Health Information shall be used or disclosed solely for such purpose or purposes which prevented the return or destruction of such Protected Health Information.

IN WITNESS WHEREOF, and intending to be legally bound, the Company affixes its signature below.

A handwritten signature in black ink, consisting of stylized, overlapping loops and a long horizontal line extending to the right.

---

By: Gregg L. Hanson  
Title: Chief Executive Officer