

BUSINESS ASSOCIATE AND DATA PROTECTION AGREEMENT BETWEEN FAIR AMERICAN INSURANCE AND REINSURANCE COMPANY AND PROFESSIONAL RISK MANAGEMENT SERVICES, INC. FOR THE POLICYHOLDERS OF THE PSYCHIATRISTS' PROGRAM AND THE NEUROLOGISTS' PROGRAM ("INSUREDS")

THIS BUSINESS ASSOCIATE AND DATA PROTECTION AGREEMENT ("the Agreement") is effective February 19, 2019 between Professional Risk Management Services, Inc., ("Business Associate Sub-Contractor" or "BAA Subcontractor") and Fair American Insurance and Reinsurance Company (hereinafter "FAIRCO" and collectively with BAA Subcontractor referred to as "Business Associates") for the benefit of the Insured.

Recitals

To the extent that the Insureds are Covered Entities ("CE") under the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), or that Business Associates have received certain information from such Covered Entities, they may have obligations concerning the privacy and security of Protected Health Information ("PHI"). One of these obligations may be to ensure that Business Associates to which the Covered Entities provide such PHI enter into a Business Associate Agreements ("BAA") and Business Associates that provide PHI to their Sub-Contractor enter into Business Associate Agreements and such BAAs set out the terms under which the Subcontractor Business Associate will collect, store or use PHI provided by the Covered Entities to the Business Associate. In addition, certain federal, state and local laws protect the privacy, use, and security of certain Personal Information ("PI") related to individuals which must be used for the purposes for which it was collected and protected from unauthorized use or disclosure as well.

To the extent that the Insureds operate a drug and alcohol treatment program that must comply with the federal Confidentiality of Substance Use Disorder Patient Records law and regulations, 42 USC § 290dd-2 and 42 CFR Part 2 (collectively, "Part 2"), Business Associates are also Qualified Service Organizations ("QSOs") under Part 2 and agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment records.

The Business Associate Sub-Contractor may collect, store or use PHI or PI provided by the Business Associate or Covered Entities for the purpose of the Provision of Insurance Coverage, as defined below.

The Business Associate agrees as follows:

I. Definitions

Catch-all definition:

The following terms used in this Agreement, as they relate to the disclosure, storage, use, processing or transmittal of Protected Health Information (PHI) shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

In addition, the term "Privacy Data" shall include all information protected from disclosure by applicable international, federal, state or local data privacy or data protection statutes, and shall include "personal information" or "personal data" as defined by applicable laws, Nonpublic Information as defined in Section 500.01(g) of New York State Department of Financial Services 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies, Protected Health Information (PHI) or electronic Protected Health Information (ePHI) as described in the Health Insurance Portability and Accountability

Act of 1996 (Pub.L. 104-191, 110 Stat. 1936 and Health Information Technology for Economic and Clinical Health (HITECH) Act) and rules and regulations adopted thereto (collectively, "HIPAA"), Payment Card Information ("PCI"), or other information protected from disclosure by Gramm Leach Bliley Act ("GLBA"), the FTC Act, the Fair Credit Reporting Act ("FCRA") or any other applicable federal, state or other law or regulation. The reference to these statutes are meant to be by example only, and neither admit that such statutes apply to the data to be transferred, nor are intended to constitute a comprehensive list of privacy statutes which may apply to the transfer of data. As it pertains to this agreement, the term Privacy Data means that information relating to FAIRCO, its clients, customers, insured, employees or related individuals, and the applicable data security regulations that relate to those computers, networks, routers, firewalls, software or devices which could impact the privacy and/or security of such data. With respect to cloud services, this includes any portion of the cloud, or any shared hardware or software service of other functionality delivered "as a service" which could impact the privacy or security of such Privacy Data.

Specific definitions:

(a) Company. "Company" as it relates to PHI and ePHI shall generally have the same meaning as the term "Business Associate" as defined in 45 CFR 160.103, and in reference to the party to this agreement, shall mean the BAA Sub-Contractor (Professional Risk Management Services, Inc.). As it relates to other Privacy Data, the term means the party receiving such information.

(b) FAIRCO. "FAIRCO" shall generally mean the entity disclosing or transferring PHI or Privacy Data, and for the purposes of this agreement means Fair American Insurance and Reinsurance Company. For convenience of definition, the parties may reference the definitions of "Covered Entity" in the HIPAA Rules with respect to PHI, even though FAIRCO is not such a Covered Entity.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) Privacy Rules: "Privacy Rules" shall mean any law, regulation, or binding legal decision impacting the privacy or security of data, and shall include, without limitation, state or local data breach disclosure laws, credit monitoring laws, and data security requirements.

II. Obligations and Activities of Company

Company agrees to:

(a) Not use or disclose Protected Health Information or Privacy Data other than as permitted or required by this Agreement or as required by law;

(b) Use appropriate safeguards, pursuant to a written information security policy, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, and any other applicable safeguards or Privacy Rules, to prevent use or disclosure of Protected Health Information or Privacy Data other than as provided for by the Agreement including conducting an independent security assessment of its safeguards by a qualified third party at least annually, and responding effectively to the findings of such independent assessment. Company's written information security program shall, at a minimum: (1) designate one or more employees to coordinate the security program; (2) identify "reasonably foreseeable" internal and external risks to the security and

confidentiality of Privacy Data and customer information that could lead to unauthorized disclosure, use, alteration, destruction or other compromise of such information and “assess the sufficiency” of the Company’s safeguards in place to control these risks. Such risk assessment must include, at a minimum, risks in areas of operation such as: (a) employee training and management, (b) information systems, and (c) detecting, preventing, and responding to attacks against Company’s systems; (3) implement safeguards to manage the identified risks and regularly test or monitor such safeguards; (4) oversee Company’s service providers by: (a) selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and (b) requiring service providers by contract to implement and maintain such safeguards; and (5) evaluate and adjust Company’s security program in light of such risk assessment, any material change to Company’s business operations, or any other circumstances that may have a material impact on its information security program.

(c) Report to FAIRCO any use or disclosure of Protected Health Information or Privacy Data not provided for by the Agreement of which it becomes aware, including breaches of unsecured Protected Health Information as required at 45 CFR 164.410, and any security incident of which it becomes aware or which it reasonably suspects. Company shall notify FAIRCO as soon as possible (but in any event within forty-eight (48) hours) of discovery or suspicion of when the Company learns of such occurrence. Company shall report within three (3) business days of the notice to FAIRCO identifying: (a) the nature of the unauthorized use or disclosure/Security Incident; (b) the PHI or Privacy Data or used or disclosed; (c) who made the unauthorized use or received the unauthorized disclosure; (d) what Company has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure (e) what corrective action Company has taken or shall take to prevent future similar unauthorized use or disclosure; and (f) any other such information, including a written report, as reasonably requested by FAIRCO.

- i. With respect to the reporting of any security incident(s), as referenced above, the parties stipulate and agree that Company will furnish the required report to FAIRCO in all cases involving a “Successful Security Incident,” which is defined for purposes of this Agreement as any security incident that results in unauthorized access, use, disclosure, modification or destruction of electronic Protected Health Information of FAIRCO or interference with system operations adversely affecting the ability of Company to maintain, process or safeguard electronic Protected Health Information or Privacy Data of FAIRCO. The parties further stipulate and agree that this paragraph constitutes notice by Company to FAIRCO with respect to any Unsuccessful Security Incident, which is defined for purposes of this Agreement as any security incident that does not result in unauthorized access, use, disclosure, modification or destruction of electronic Protected Health Information or Privacy Data of FAIRCO or interference with system operations adversely affecting the ability of Company to maintain, process or safeguard electronic Protected Health Information or Privacy Data of FAIRCO. By way of example, such Unsuccessful Security Incidents may include: (i) pings on the firewall of Company; (ii) port scans; (iii) attempts to log on to a system or enter a database with an invalid password or username; (iv) denial-of-service attacks that do not result in a server being taken off-line; and/or (v) malware (worms, viruses, etc.). The parties further stipulate and agree that with respect to any such Unsuccessful Security Incident, no further or more detailed report to FAIRCO is needed or required under this Agreement.

- ii. In the event of an unauthorized disclosure, use or Breach of PHI or Privacy Data that is in the custody or control of Company, Company will take the following steps to assist FAIRCO in addressing applicable requirements under the HIPAA Rules or relevant data breach notification requirements or Privacy Rules, and to assist FAIRCO in fulfilling FAIRCO's HIPAA or other breach notice obligations. Within three (3) business days, Company agrees to provide:
 - a. Company's initial assessment and opinion regarding whether a particular unauthorized data release incident constitutes a "Breach" that triggers the HIPAA or other breach notification requirements; and
 - b. Company's initial risk assessment and opinion regarding level of risk associated with the breach and/or security incident; and
 - c. Company agrees to provide FAIRCO with copies of all materials and information disclosed so that FAIRCO can perform independent risk assessment; and
 - d. Where notifications are required, Company agrees to provide assistance in drafting proposed notification(s) to the affected individuals, HHS/OCR, state or local government officials, law enforcement officials, or prominent media outlets. However, FAIRCO, in its sole discretion, will make final determination and be responsible for notification of individuals, HHS/OCR, other government officials, and media if required; and
 - e. Company will provide assistance to FAIRCO in the form of supplying data in the possession of the Company that is needed by FAIRCO to make the annual report to HHS/OCR of data breach incidents, as required under the HIPAA Rule, or such information disclosure or reporting requirements. Company agrees to work cooperatively with FAIRCO to help FAIRCO fulfill the annual HHS/OCR log or reporting requirement or other reporting requirements. Company shall be responsible for all costs reasonably associated with the investigation and mitigation of harm or damages resulting from such security incident, including but not limited to costs of forensic or other investigation, assessment, data breach notification, data breach remediation, credit monitoring, repair or freeze, regulatory or other investigation or fines, and shall indemnify and hold FAIRCO harmless for any costs and/or claims resulting directly or indirectly from any such breach and/or noncompliance with applicable laws and regulations, including attorney's fees associated with such claims.

(d) Ensure that any subcontractors that create, receive, use, maintain, or transmit Protected Health Information or Privacy Data on behalf of the Company agree to the same restrictions, conditions, and requirements that apply to the Company with respect to such information;

(e) Make available Protected Health Information or Privacy Data in a designated record set to the "individual or the individual's designee" as necessary to satisfy FAIRCO's obligations under 45 CFR 164.524;

(f) Make any amendment(s) to Protected Health Information or Privacy Data in a

designated record set as directed or agreed to by FAIRCO pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy FAIRCO's obligations under 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to the "individual" as necessary to satisfy FAIRCO's obligations under 45 CFR 164.528;

(h) To the extent the Company is to carry out one or more of FAIRCO's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to FAIRCO in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules, and make them available to FAIRCO if required for compliance with relevant Privacy Rules.

III. Qualified Service Organization (QSO) Responsibilities

To the extent that in performing services Business Associates use, disclose, maintain, or transmit information protected by Part 2, Business Associates acknowledge and agree that they are QSOs for the purpose of such federal law, acknowledge and agree that in receiving, storing, processing or otherwise dealing with any such patient records, they are fully bound by the Part 2 regulations; and, if necessary, will resist in judicial proceeding any efforts to obtain access to patient records except as permitted by the Part 2 regulations.

IV. Permitted Uses and Disclosures by Company

(a) Company may only use or disclose Protected Health Information or Privacy Data as otherwise limited in this Agreement: Company may use or disclose Protected Health Information or Privacy Data it creates or receives to perform functions, activities, or services for, or on behalf of, FAIRCO, provided that such use or disclosure would not violate HIPAA or other Privacy Rules if done by FAIRCO or the minimum necessary policies and procedures of FAIRCO.

(b) Company may request additional use of FAIRCO's data by specific request, which will be reviewed and approved in writing on an individual basis and added as an addendum to this agreement

(c) Company may not release or use for its own purposes, FAIRCO's data, even in de-identified format (45 CFR 164.514(a)-(c)) without a written request and written authorization from FAIRCO.

(d) Company may use or disclose Protected Health Information or Privacy Data as required by law but only with the advance consent of FAIRCO.

(e) Company agrees to make uses and disclosures and requests for Protected Health Information or Privacy Data consistent with FAIRCO's minimum necessary policies and procedures.

(f) Company may not use or disclose Protected Health Information or Privacy Data in a

manner that would violate Subpart E of 45 CFR Part 164 or other privacy law or regulation if done by FAIRCO, except for the specific uses and disclosures set forth below.

(g) Company may use Protected Health Information or Privacy Data for the proper management and administration of the Company or to carry out the legal responsibilities of the Company, provided that doing so does not compromise the security or confidentiality of such data and such data is not used for other unrelated business enrichment purposes unless such use has been given prior written approval by FAIRCO

(h) Company will not release Protected Health Information or Privacy Data pursuant to subpoena or other demand, without first providing FAIRCO notice and an opportunity to challenge such subpoena or demand.

(i) Except as otherwise limited in this Agreement, Company may provide data aggregation services relating to insurance underwriting or processing of FAIRCO, with de-identified information as permitted by 45 CFR - 164.504(e)(2)(i)(B).

V. **Provisions for FAIRCO to Inform Company of Privacy Practices and Restrictions**

(a) FAIRCO shall notify Company of any limitation(s) in the notice of privacy practices of FAIRCO under 45 CFR 164.520, or other Privacy Rules to the extent that such limitation may affect Company's use or disclosure of Protected Health Information or Privacy Data.

(b) FAIRCO shall notify Company of any changes in, or revocation of, the permission by an individual to use or disclose his or her Protected Health Information and/or Privacy Data, to the extent that such changes may affect Company's use or disclosure of Protected Health Information and/or Privacy Data.

(c) FAIRCO shall notify Company of any restriction on the use or disclosure of Protected Health Information and/or Privacy Data that FAIRCO has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Company's use or disclosure of Protected Health Information and/or Privacy Data.

VI. **Permissible Requests by FAIRCO**

FAIRCO shall not request Company to use or disclose Protected Health Information or Privacy Data in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by FAIRCO.

VII. **Term and Termination**

(a) **Term**. This Agreement shall terminate when all of the Protected Health Information and/or Privacy Data provided by FAIRCO to Company, or created or received by Company on behalf of FAIRCO, is destroyed or returned to FAIRCO, or, if it is infeasible to return or destroy Protected Health Information and/or Privacy Data, protections are extended to such information, in accordance with the termination

provisions in this Section, or on the date FAIRCO terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Upon FAIRCO's knowledge of a material breach by Company, FAIRCO shall either:

1. Provide an opportunity for Company to cure the breach or end the violation and terminate this Agreement (and any management or other such agreement to which this Agreement relates) if Company does not cure the breach or end the violation within the time specified by FAIRCO;
2. Immediately terminate this Agreement (and any management or other such agreement to which this Agreement relates) if Company has breached a material term of this Agreement and cure is not possible; or
3. If neither termination nor cure is feasible, FAIRCO shall report the violation to the Secretary.
4. Notwithstanding the foregoing, FAIRCO may terminate this Agreement (and any management or other such agreement to which this Agreement relates) for cause in the event of an actual or suspected data breach or a significant security event, irrespective of whether: (a) such event resulted in a data breach involving FAIRCO or its customers Protected Health Information or Privacy Data, (b) such event occurred as a result of the actions or omissions of Company, or (c) such event occurred as a result of the actions or omissions of any third party.

(c) Obligations of Company Upon Termination.

Upon termination of this Agreement for any reason, Company, with respect to Protected Health Information or Privacy Data received from FAIRCO, or created, maintained, or received by Company on behalf of FAIRCO, shall:

1. Continue to: (i) provide services and fulfill obligations as set forth in any FAIRCO agreements; (ii) abide by the requirements in this Agreement; (iii) use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 or other privacy or data security law applicable, with respect to electronic Protected Health Information and/or Privacy Data to prevent use or disclosure of the Protected Health Information or Privacy Data, for as long as Company retains the Protected Health Information and/or Privacy Data; and (iv) not use or disclose the Protected Health Information and/or Privacy Data retained by Company other than for the purposes for which such Protected Health Information and/or Privacy Data was retained and subject to the same conditions set out at in section III "Permitted Uses and Disclosures By Company" which applied prior to termination.
2. At FAIRCO's direction, return to FAIRCO or destroy the remaining Protected Health Information and/or Privacy Data that the Company still maintains in any form. Protected Health Information or Privacy Data shall be securely destroyed in accordance with industry best practices for shredding of physical documents and wiping of electronic media (e.g., National Institute of Standards

and Technology Special Publication 800-88). Promptly following any destruction hereunder Company shall provide a written confirmation by a duly authorized senior employee regarding completion and compliance with the destruction requirements set forth herein.

(d) Survival. The obligations of Company under this Section shall survive the termination of this Agreement.

VIII. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended. A reference to applicable Privacy Rules shall mean such rules as in effect or amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules, Privacy Rules, and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules, Privacy Rules, or any other applicable law.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on behalf effective as of February 19, 2019.

BY FAIRCO

Professional Risk Management Services, Inc.

By: _____

By: _____

Print Name: Regan Adams

Print Name: Donna Vanderpool

Print Title: Chief Financial Officer

Print Title: VP, Risk Management

Signature: 

Signature: 

Date: 3-14-19

Date: 2/19/19