



## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (Business Associate Agreement”) effective as of the Effective Date of the Services Agreement, is entered into by and between \_\_\_\_\_ (“Business Associate”) and McGregor (“Covered Entity”).

### RECITALS

WHEREAS, Business Associate has entered into that certain Services Agreement (“Agreement”) pursuant to which Business Associate provides \_\_\_\_\_ to Covered Entity and in furtherance of such Agreement, Business Associate may from time to time perform on behalf of Covered Entity a function or activity supporting the Covered Entity that involves the Use or Disclosure of Protected Health Information (“PHI”).

WHEREAS, Business Associate and Covered Entity desire to enter into this Business Associate Agreement regarding the Use and/or Disclosure of PHI as required by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), THE Standards for Privacy of Individually Identifiable Health Information (the “Privacy Rule”) and the Standards for Security of Electronic Protected Health Information (the “Security Rule”) promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII and Division B, Title IV, of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5) (the “HITECH Act”), and the regulations implementing the HITECH Act.

NOW, THEREFORE, in consideration of the mutual promises below and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

### AGREEMENT

#### A. General Compliance with HIPAA Privacy Rule and Security Rule.

The parties shall conduct their respective businesses in accordance with all applicable laws and regulations regarding the privacy and security of PHI, including, without limitation, HIPAA and the HITECH Act, as amended from time to time, and the regulations promulgated thereunder.

#### B. Definitions.

Terms used but not otherwise defined in this Business Associate Agreement shall have the same meaning given to such terms in HIPAA, the HITECH Act, or any implementing regulations promulgated thereunder, including, but not limited to, the Privacy Rule and the Security Rule, the definitions in HIPAA, the HITECH Act and any implementing regulations shall govern.

1. “Breach” means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of PH (within the meaning of 45 C.F.R. § 164.402).
2. “Data Aggregation” means, with respect to PHI created or received by Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.
3. “Designated Record Set” means a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For the purposes of this paragraph, the term “record” means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a covered entity.
4. Disclose or Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.
5. “Electronic Protected Health Information or ePHI” shall have the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
6. “Individual” means the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
7. “Individually Identifiable Health Information” means information that is a subset of health information, including demographic information collected from an Individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or

future physical or mental health or condition of an Individual; the provision of health care to an Individual; and (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

8. “Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
9. “Protected Health Information” or “PHI” means Individually Identifiable Health Information that is: (i) transmitted by “electronic media”, as defined in 45 C.F.R. § 160.103; (ii) maintained in any medium described in the definition of electronic media; or (iii) transmitted or maintained in any other form or medium.
10. “Required by Law” means a mandate contained in law that compels an entity to make a Use or Disclosure of PHI and that is enforceable in a court of law.
11. “Secretary” means the Secretary of Health and Human Services or any other officer or employee of the U.S. Department of Health and Human Services to whom the authority involved has been delegated.
12. “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.
13. “Security Rule” means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164 Subpart C.
14. “Unsecured Protected Health Information” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.
15. “Use” means the sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information.

C. Obligations and Activities of Business Associate.

1. Nondisclosure. Business Associate shall not Use or Disclose PHI other than as permitted or required by the Agreement, this Business Associate Agreement, or as Required by Law.
2. Minimum Necessary. Business Associate shall limit any PHI Used, Disclosed or requested to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or request.
3. Safeguards. Business Associate shall use appropriate safeguards to prevent the Use or Disclosure of PHI other than as provided for the Agreement or this Business Associate Agreement.
4. Security Rule. Business Associate shall comply with the Security Rule provisions set forth in 45 C.F.R. Part 164, Subpart C, including the provisions relating to Security Standards General Rules (45 C.F.R. § 164.306), Administrative Safeguards (45 C.F.R. § 164.308), Physical Safeguards (45 C.F.R. § 164.310), Technical Safeguards (45 C.F.R. § 164.312), Organizational Requirements (45 C.F.R. § 164.314) and Policies Documentation (45 C.F.R. § 164.316), and to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.
5. Certification. To the extent that Covered Entity determines that such examination is necessary to comply with Covered Entity's legal obligation pursuant to HIPAA relating to certification of its security practices, Covered Entity or its authorized agents or subcontractors, may at Covered Entity's expense, examine Business Associate's facilities, security risk assessment, policies & procedures, employee training requirements, employee files and other systems. Procedures and records as may be necessary for such agents or contractors to certify to Covered Entity the extent to which Business Associate's security safeguards comply with HIPAA, the HITECH Omnibus Rule, the HIPAA Regulations or this Agreement. Business Associate is required to complete Attachment "A" – "Business Associates Compliance Status Questionnaire" as part of this Agreement.
6. Reporting of Disclosures. Business Associate shall report directly to Covered Entity, in writing, any Use or Disclosure of PHI that comes to the attention of Business Associate that is not permitted or provided for by the Agreement or this Business Associate Agreement.

7. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Business Associate Agreement.
8. Business Associate's Agents. Business Associate shall ensure that any agents, including subcontractors, which create, receive, maintain or transmit PHI on behalf of Business Associate agree in writing to restrictions and conditions that are no less restrictive than those that apply to Business Associate through this Business Associate Agreement with respect to PHI.
9. Access to PHI. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity), Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity in writing, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. This provision shall only apply if Business Associate has PHI in a Designated Record Set. Business Associate further shall notify Covered Entity of any requests for access it receives from an individual within five (5) business days of receipt.
10. Documentation of Disclosures. Business Associate shall document such Disclosures of PHI and information related to such Disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528.
11. Accounting Disclosures. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity), Business Associate shall provide to Covered Entity information collected in accordance with Section C.9 of this Business Associate Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528 (and HITECH Act § 13405(c) when such requirements are effective as to any covered entity with whom Covered Entity maintains an Agreement). Business Associate further shall notify Covered Entity of any requests for accounting of Disclosures it receives from an Individual within ten (10) business days of receipt.

12. Amendment of PHI. At the written request of Covered Entity (and in the reasonable time and manner designated by Covered Entity), Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs pursuant to 45 C.F.R. § 164.526. This provision shall only apply if Business Associate has PHI in a Designated Record Set. Business Associate further shall notify Covered Entity of any requests for amendment it receives from an Individual within fifteen (15) business days of receipt.
13. Internal Practices. Business Associate shall make its internal practices, books, and records, including policies and procedures, relating to the Use and Disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or to the Secretary, for purposes of determining Covered Entity's and/or Business Associate's compliance with the Privacy and/or Security Rule.
14. Reporting of Potential Breaches and Security Incidences. Business Associate shall report in writing to Covered Entity any Security Incident or potential Breach or Unsecured Protected Health Information as follows:
- a) Business Associate shall report any actual, successful Security Incident within fifteen (15) days of Business Associate's discovery of such actual, successful Security Incident.
  - b) Business Associate shall report any attempted, unsuccessful Security Incident of which Business Associate becomes aware at the written request of Covered Entity but in no event less frequently than on a quarterly basis.
  - c) Business Associate shall report any potential Breach of Unsecured Protected Health Information within two (2) days of discovery.

In each instance (a) through (c) above, the written report shall include the following: (i) 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 during any such Security Incident or potential Breach, to the extent known by Business Associate; (ii) such other information regarding the Security Incident or potential Breach as is known to Business Associate at the time the report is made (such as the type of PHI involved, the nature of the information accessed, acquired, Used or Disclosed, etc.); (iii) an acknowledgement by Business Associate that the information provided pursuant to (i) and (ii) shall be supplemented if and when further information becomes available to Business Associate.

15. Additional Responsibility. To the extent Business Associate is to carry out an obligation of Covered Entity under the Privacy Rule provisions set forth at 45 C.F.R. Part 164, Subpart E, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

D. Permitted Uses and Disclosures by Business Associate.

1. Permitted Uses and Disclosures. Except as otherwise limited in this Business Associate Agreement, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement, provided such Use or Disclosure would not violate the Privacy Rule if done by Covered Entity.
2. Use for Management and Administration. Except as otherwise limited in this Business Associate Agreement, Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
3. Disclosure for Management and Administration. Except as otherwise limited in the Agreement and this Business Associate Agreement, Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that: (a) the Disclosures are Required by Law, or (b) Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and (c) the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
4. Data Aggregation. Except as otherwise limited in this Business Associate Agreement, Business Associate may Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

E. Obligations of Covered Entity.

1. Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices from Covered Entity, as well as any limitations and/or changes to such notice, of which Covered Entity is notified, to the extent that such limitations and/or changes may affect Business Associate's Use or Disclosure of PHI.

2. Changes in Permission. Covered Entity shall notify Business Associate of any changes in, revocation of, permission by an individual to Use or Disclose PHI, of which Covered Entity is notified, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.
3. Notification of Restrictions. Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522 and of which Covered Entity is notified, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.
4. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate Use or Disclose PHI in any manner that would not be permissible under HIPAA, as amended by the HITECH Act, or any implementing regulations.

F. Term and Terminations.

1. Term. The term of this Business Associate Agreement shall be effective as of the effective date of the Agreement and shall remain in effect until the expiration or termination of the Agreement between the parties.
2. Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement.
3. Effect of Termination. Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:
  - a. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
  - b. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
  - c. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health



information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

- d. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses
- e. Survival. The obligations of the Business Associate under this Section shall survive the termination of this Agreement.

G. Miscellaneous.

1. Regulatory References. A reference in this Business Associate Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.
2. 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 and any other applicable law.
3. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

IN WITNESS WHEREOF, the parties have signed this Agreement on the date indicated below.

MCGREGOR PACE

By: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_