

Business Associate/ Subcontractor Business Associate Agreement

This Business Associate/ Subcontractor Business Associate Agreement (“**BAA**”) forms part of the Service Agreement or other written or electronic agreement between AllCloud (“**AllCloud**”) and Customer (“**Customer**”) for the purchase of AllCloud’s Services (hereinafter referred to as the “**Services**”) as detailed in the agreement between the parties (the “**Applicable Agreement**”) to reflect the parties’ agreement with regard to the Processing of Personal Data.

By accepting or signing the Applicable Agreement, and/or accessing or using the Services, Customer enters this BAA. If you do not agree to be bound by and comply with all the terms hereof or may not have the authority on behalf of Customer, you may not access or use the Services.

1. Definitions

- 1.1. “**Applicable Data Protection Laws**” means all laws and regulations relating to e/PHI, applicable to the parties in connection with the Services and the Agreement. This may include without limitation: (a) HIPAA (as defined below); and (b) the Health Information Technology Provisions of American Recovery and Reinvestment Act of 2009 (HITECH). No law shall be considered an Applicable Data Protection Law prior to its effective date.
- 1.2. **The following terms used in this Addendum shall have the meaning ascribed thereto in the HIPAA Rules:** AllCloud, Customer, Breach, Data Aggregation, Designated Record Set, Disclosure or Disclose, Health Care Operations, Individual, Minimum Necessary Notice of Privacy Practices Required by Law, Secretary, Security Incident, Subcontractor, and Use.
- 1.3. “**Services**” means AllCloud services as may be published and provided to customers from time to time.

2. Roles of the Parties

- 2.1. When AllCloud provides services directly to Covered Entities, AllCloud shall construed as “Business Associate”.
- 2.2. When AllCloud provides services directly to Business Associate, AllCloud shall construed as Subcontractor Business Associate.
3. In the event **AllCloud** creates, receives, maintains, or otherwise is exposed to personally identifiable or aggregate patient or other medical information defined as Protected Health Information (“**PHI**”) in the Health Insurance Portability and Accountability Act of 1996 or its relevant regulations (“**HIPAA**”) and otherwise meets the definition of AllCloud as defined in the HIPAA Privacy Standards (45 CFR Parts 160 and 164), **AllCloud** shall:
 - 3.1. Not use or further disclose the PHI, except as permitted by law
 - 3.2. Not use or further disclosing the PHI in a manner that had the Customer done so, would violate the requirements of HIPAA;
 - 3.3. Use appropriate safeguards (including implementing administrative, physical, and technical safeguards for electronic PHI) to protect the confidentiality, integrity, and availability of and to prevent the use or disclosure of the PHI other than as provided for by the Applicable Agreement;
 - 3.4. Comply with each applicable requirement of 45 C.F.R. Part 162 if the AllCloud conducts Standard Transactions for or on behalf of the Customer;

- 3.5. Report promptly to the Customer any security incident or other use or disclosure of PHI not provided for by this Agreement of which AllCloud becomes aware;
- 3.6. Ensure that any subcontractors or agents who receive or are exposed to PHI (whether in electronic or other format) are explained the AllCloud obligations under this paragraph and agree to the same restrictions and conditions;
- 3.7. In certain circumstances, account for PHI disclosures for up to the past six (6) years as requested by Customer, which shall include: (i) dates of disclosure, (ii) names of the entities or persons who received the PHI, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose and basis of such disclosure;

4. Authorized Use

- 4.1. **Customer** hereby agrees that:
 - 4.1.1. **AllCloud** may de-identify and/or anonymize and/or aggregate PHI in a way that does not enable the identification of an individual and may use, share, and maintain such data as required for conducting the services.
 - 4.1.2. **AllCloud** (a) may Use or Disclose PHI as required by law; (b) agrees to make Uses Disclosures and requests for PHI consistent with Customer's Minimum Necessary policies and procedures; and (c) may not Use or Disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 of HIPAA if done by Customer except for the specific Uses and Disclosures set forth above.
 - 4.1.3. Subject to Section 12 ("Return or Destruction of Protected Health Information upon Termination"), the duration of the processing shall be for the term of the Applicable Agreement and shall apply to all of the Services and/or materials delivered by the AllCloud pursuant thereto.

5. Compliance with Laws

- 5.1. Each Party shall comply with its obligations under Applicable Data Protection laws.
- 5.2. To the extent **AllCloud** is to carry out one or more of Customer's obligation(s) under Subpart E of 45 CFR Part 164 of HIPAA, AllCloud shall comply with the requirements of Subpart E that apply to the Customer in the performance of such obligation(s).

6. Obligation of Confidentiality.

- 6.1. AllCloud shall take reasonable steps to ensure that its employees, agents and/or subcontractors shall have access to PHI on a "need to know" basis, and they signed or are otherwise legally obligated to confidentiality obligations at the similar level of the Applicable Agreement.
- 6.2. AllCloud shall train its employees on compliance with Applicable Data Protection Laws.

7. Security Measures

- 7.1. AllCloud shall, in relation to PHI, implement commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of AllCloud's business, the level of sensitivity of the data collected, handled and stored, and the nature of AllCloud's business activities ("**Security Measures**"), including, as appropriate, the following measures: (a) pseudonymisation and/or encryption of PHI; and ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- 7.2. AllCloud shall Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 of HIPAA with respect to ePHI, to prevent Use or Disclosure of PHI other than as provided for by the Applicable Agreement.

8. Assistance with Safeguarding Individual Rights. Taking into account the scope and nature of the Services, AllCloud shall Assist the Customer with exercise Individual Rights.

9. Breach Incidents

- 9.1. No later than 30 days from the discovery of the Breach after becoming aware thereof, AllCloud will notify Customer and will provide information known to it at such time with respect to the nature, scope and consequences of such Breach Incident.
- 9.2. AllCloud will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Breach Incident.
- 9.3. AllCloud's obligations under this Section shall not apply to Breach Incidents that are caused by Customer.
- 9.4. Taking into account the scope and nature of the services, Upon reasonable notice, AllCloud shall provide reasonable assistance to Customer in compliance with any notification obligations of Breach Incidents to the supervisory as required under the Applicable Data Protection Laws.

10. Security Assessments and Audits

- 10.1. AllCloud shall, upon reasonable and written notice and subject to obligations of confidentiality, allow its data processing policies to be inspected annually by a third party (that is subject to confidentiality agreement) to be agreed upon between AllCloud and Customer to ascertain compliance with this Agreement. The costs of such an inspection shall be borne by Customer.
- 10.2. AllCloud shall make its internal practices, books, and records that are only relevant to the provided services, available to the U.S. Secretary of Health and Human Services for purposes of determining AllClouds compliance with HIPAA Rules.

11. Sub-Processors

- 11.1. Unless otherwise prohibited in the Applicable Agreement, Customer agrees that AllCloud may engage sub-processors to perform its obligations under the Applicable Agreement, provided that they agree to process PHI in a manner consistent with and no less protective of Customer and/or the terms of this BAA, and provided that AllCloud remains liable for the acts and omissions of such sub-processors. A list of sub-processors may be provided upon Customer's request.

12. Term and Termination

- 12.1. This Agreement shall remain in effect for the duration of the Applicable Agreement and shall apply to the Services delivered by Customer pursuant to the Applicable Agreement.
- 12.2. Termination for Cause. Each party may terminate this Agreement for cause if they determine the other party has violated a material term of this Addendum and such party has not cured the breach or ended the violation within reasonable time of not less than 30 days.

13. Return or Destruction of Protected Health Information upon Termination.

- 13.1. Upon the termination of this Agreement, unless otherwise directed by Customer, AllCloud shall either return or destroy, and instruct its sub-processors to return or destroy all PHI received from the Customer or created or received by AllCloud on behalf of the Customer in which AllCloud maintains in any form. AllCloud shall not retain any copies of such PHI.
- 13.2. Notwithstanding the foregoing, in the event that AllCloud determines that returning or destroying the Protected Health Information is infeasible upon termination of this Agreement, AllCloud shall provide to Customer notification of the condition that makes return or destruction infeasible. To the extent that it is not feasible for AllCloud to return or destroy such

PHI, the terms and provisions of this Agreement shall survive such termination or expiration and such PHI shall be used or disclosed solely as permitted by law for so long as AllCloud maintains such Protected Health Information.

- 13.3. Notwithstanding the foregoing, AllCloud may retain PHI to the extent and for such period as required: (a) by applicable laws; (b) for the purpose of defending itself against legal claims; and (c) to continue its proper management and administration or to carry out its legal responsibilities. During such time, AllCloud shall not process such PHI other than for the purposes set forth above and subject to the same conditions set out in this BAA. AllCloud shall return or destroy to Customer such PHI when it is no longer needed for the above purposes.

14. Miscellaneous

- 14.1. Survival. Provisions which by their nature are intended to survive the suspension or termination of this BAA shall survive its termination.
- 14.2. Should any provision of this BAA be invalid or unenforceable, then the remainder of this BAA shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.
- 14.3. Any claims brought in connection with this BAA will be subject to the terms of the Applicable Agreement.
- 14.4. AllCloud may update the terms of this BAA from time to time.