BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("BAA") is effective as of the date of last signature below ("Effective Date"), by and between ClicData a corporation with offices at 459 Columbus Ave #4007, New York NY 10024 ("Vendor" or "Business Associate"), and _____ the Covered Entity Corporation ("Covered Entity") with offices at _____ (each a "Party" and collectively the "Parties).

1. Background

1. Covered Entity is using the platform provided by the Business Associate to store and manage data.
2. Covered Entity receives and maintains Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the regulations promulgated thereunder by the United States Department of Health and Human Services at 45 CFR 160 to 164 (collectively, "HIPAA") on behalf of its clients that are subject to HIPAA ("Clients"), and is permitted to use or disclose such Protected Health Information only in accordance with HIPAA.
3. ClicData provides a data analytics and management platform that is customer-controlled and content-neutral. As such, ClicData does not access, monitor, or validate the content of data uploaded by the customer, including whether such data qualifies as Protected Health Information (PHI) under HIPAA. The Covered Entity is solely responsible for determining the nature of the data processed through the platform and for ensuring that any PHI is handled in compliance with HIPAA requirements. ClicData's role as a Business Associate shall apply only where PHI is knowingly and explicitly disclosed to ClicData for support, implementation, or contracted services.
4. To the extent Vendor is deemed a "Business Associate", Vendor agrees to comply with the terms of this BAA.

2. Definitions.

Terms used but not otherwise defined in this BAA shall have the same meaning given to those terms under HIPAA.

3. Obligations and Activities of Business Associate.

Business Associate agrees to comply with the requirements of HIPAA and HITECH, including, without limitation, the Privacy and Security Rules.

Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this BAA, the Privacy and Security Rules, as necessary under the Agreement, or as required by law. Such disclosures shall be consistent with the "minimum necessary" requirements of the Regulations.

Business Associate agrees to use appropriate administrative, technical and physical safeguards and to comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information to prevent the use or disclosure of Protected Health Information other than as provided for by this BAA or in connection with the Agreement.

Upon request, Business Associate shall provide a list of all subcontractors it engages under the Agreement which may have access to PHI, which shall be sent to.

Business Associate agrees to require any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity to agree in writing to the same restrictions and conditions on the use, disclosure and/or protection of PHI that apply through this BAA to Business Associate with respect to such information in accordance with § 164.502(e) (1) (ii) and § 164.308(b) (2) of HIPAA.

Business Associate shall not be required to grant Covered Entity or its Clients physical access to its facilities or systems. Instead, Business Associate shall make available, upon reasonable written request, relevant documentation demonstrating its compliance with applicable HIPAA obligations, including third-party audit reports (e.g., SOC 2, ISO 27001), internal security policies, and summaries of controls. Any such disclosures shall be limited to what is reasonably necessary to assess compliance and shall not include access to multi-tenant infrastructure, proprietary systems, or other customer environments. Business Associate may require execution of a confidentiality agreement prior to releasing such materials.

Business Associate agrees to provide to Covered Entity or Client, in time and manner reasonably designated by Covered Entity, information collected in accordance with Section 2(i) of this BAA, to permit Client to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with § 164.528 of HIPAA.

To the extent Business Associate agrees to undertake an obligation of Covered Entity or Client under HIPAA, Business Associate will comply with the applicable requirements of HIPAA in the performance of such obligation.

4. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information as expressly necessary to perform the functions, activities or services for, or on behalf of, Covered Entity or Client as set forth in the Agreement, or as otherwise Required by Law.

Except as otherwise expressly limited in this BAA, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

Except as otherwise expressly limited in this BAA, Business Associate may disclose Protected Health Information to third parties as Required By Law, or if Business Associate first obtains reasonable, written 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 the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Business Associate does not perform Data Aggregation or De-identification of Protected Health Information on behalf of the Covered Entity unless expressly agreed in writing. Any such activities, if required, must be explicitly scoped and contracted as part of the underlying service agreement. ClicData provides a self-service analytics platform where customers independently control data inputs and outputs, including aggregation, transformation, or de-identification activities. Accordingly, Business Associate shall not be deemed to have engaged in Data Aggregation or De-identification under HIPAA merely by virtue of the Covered Entity or its users using the platform's features to manipulate or visualize their own data.

Business Associate may not de-identify Protected Health Information, absent Covered Entity's prior written consent, and then, only in accordance with 45 CFR § 164.514.

Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j) (1).

5. Obligations of Covered Entity.

Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of a Client under 45 CFR § 164.520 to the extent that Covered Entity is aware of the limitation and such limitation(s) may affect Business Associate's use of disclosure of PHI.

To the extent known by Covered Entity, Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI to the extent that such changes may affect Business Associate's use or disclosure of PHI and to the extent such changes or revocations are shared with Covered Entity.

To the extent known by Covered Entity, Covered Entity shall notify Business Associate of any restriction(s) on the use or disclosure of PHI that a Client has agreed to or is required to abide by under 45 CFR § 164.522 to the extent that such restriction(s) may affect Business Associates use or disclosure of PHI.

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR § 164 if done by Covered Entity.

Covered Entity shall only request or provide Business Associate the minimum amount of PHI necessary for Business Associate to provide services under the applicable underlying Agreement and in accordance with the requirements of HIPAA and all other applicable rules relating to the privacy of PHI and related data.

6. Privacy Obligation Breach and Security Incidents.

Business Associate will promptly notify Covered Entity any Security Incident, use or disclosure of Covered Entity's Protected Health Information in violation of this BAA of which it becomes aware, including any Breaches of PHI. Business Associate will provide notification to the Covered Entity without unreasonable delay, but in no event later than forty-eight (48) hours following discovery, of such unauthorized use or disclosure of Protected Health Information. Business Associate shall reasonably cooperate with Covered Entity in investigating the Breach and in reasonably assisting with Covered Entity's and Clients' obligations under the Breach Notification Regulation of HIPAA.

In addition, following the notification referenced above, the Business Associate shall provide supplemental reports to Covered Entity as soon as additional information becomes available and no less than 10 days, including:

a) the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed
b) the nature of the non-permitted access, use or disclosure, including the date of the Breach and the date of discovery of the Breach;
c) categories of Protected Health Information accessed, used or disclosed as part of the Breach (e.g., full name, social security number, date of birth, etc.);
d) who made the non-permitted access, use or disclosure and who received the non-permitted disclosure;
e) what corrective action Business Associate did or will do to protect against further Breaches;
f) what Business Associate did or will do to mitigate the harm of any such Breach of Unprotected Health Information; and
g) such other information, including a written report, as Covered Entity may reasonably request, including in order to comply with the Breach Notification Regulation of HIPAA.

Business Associate agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this BAA or applicable law.

For Security Incidents that do not result in unauthorized access, use, disclosure, modification or destruction of information or interference with Business Associate's system operations ("Unsuccessful Security Incidents"), each party agrees that this paragraph constitutes notice from Business Associate to Covered Entity of types of such Unsuccessful Security Incidents. The parties consider the following to be illustrative, but not inclusive, of Unsuccessful Security Incidents when they do not result in unauthorized access, use, disclosure, modification, or destruction of e-PHI or interference with an information system:

- Pings on Business Associate's firewall;
- Port scans;
- Attempts to log on to a system or enter a database with an invalid password or username;
- Denial-of-service attacks that do not result in a server being taken off-line; and
- Malware (e.g., worms, viruses)

Any reports or notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to Covered Entity, to:

<enter information>

If to Business Associate, to:

ClicData
459 Columbus Ave #4007
New York NY 10024
United States
compliance@clicdata.com

7. Termination.

Except as otherwise provided herein, this BAA shall terminate upon termination of the Agreement.

8. Termination for Cause.

Upon either party's knowledge of a material breach by the other party of this BAA, the non-breaching party will:

- Notify the breaching party of such breach and provide a reasonable opportunity for the breaching party to cure the material breach or end the material violation, and if the breaching party does not cure the material breach or end the material violation within thirty (30) days or other cure period agreed upon by the parties, the non-breaching party may terminate this BAA; or
- If the breaching party has breached a material term of this BAA and cure is not possible, immediately terminate this BAA

9. Effect of Termination.

Except as provided in paragraph (2) of this section, upon termination of this BAA, for any reason, Business Associate shall, upon written request by Covered Entity, assist in the return or destruction of any Protected Health Information (PHI) that was knowingly and explicitly provided to Business Associate by Covered Entity for support, onboarding, or contracted services. ClicData is a content-neutral, self-service platform and does not monitor, access, or validate customer data stored within the platform; therefore, the Covered Entity is solely responsible for managing and removing any PHI stored in its account prior to termination. Business Associate shall not be required to return or destroy PHI that is unknown to it, resides in system logs, or is retained in encrypted backups maintained for business continuity purposes. Any such residual data shall remain subject to the confidentiality and security obligations of this BAA for as long as it is retained.

In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity prompt written notification of the conditions that make return or destruction infeasible. In the event Covered Entity agrees that return or destruction is infeasible, then Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. Except as provided herein, any termination of the maintenance program or provisions of the Agreement that permit Business Associate to access Protected Health Information shall not affect the parties other obligations or rights under the Agreement.

Notwithstanding anything to the contrary, a Breach of Unsecured PHI shall constitute a material, breach of the Agreement and shall, in Covered Entity's discretion, be grounds for immediate termination of this BAA and the Agreement for cause.

10. Changes to HIPAA.

If the HIPAA statutes or regulations are amended in a manner that would alter the obligations of Covered Entity as set forth in this BAA, then the parties agree in good faith to negotiate mutually acceptable changes to the terms set forth in this BAA. In the event the parties are unable to agree upon a written amendment satisfactory to both parties, then

notwithstanding anything to the contrary, Covered Entity shall have the right to terminate this BAA, and the Agreement, immediately and without penalty.

11. Survival.

The respective rights and obligations of Business Associate under Section 5(c) of this BAA shall survive the termination of this BAA.

12. Assignment.

Assignment shall be as set forth in the Agreement.

13. Reimbursement.

Business Associate shall reimburse Covered Entity only for actual, reasonable, and documented costs directly resulting from a Breach of Unsecured PHI or Security Incident caused solely by Business Associate's proven gross negligence or willful misconduct. Such reimbursement shall not extend to costs arising from data or system mismanagement by the Covered Entity, including inadequate security controls, improper data classification, or failure to restrict user access.

Business Associate shall not be responsible for reimbursing costs related to notification, mitigation, or credit monitoring unless it is conclusively established that the Breach was directly caused by Business Associate's failure to comply with its express obligations under this BAA. Any reimbursement shall be subject to a cap equal to the total fees paid by the Covered Entity to Business Associate in the twelve (12) months preceding the incident and shall exclude indirect, speculative, or punitive damages.

14. Indemnification.

Business Associate shall only be responsible for Breaches of Unsecured PHI or Security Incidents to the extent such incidents are the direct result of Business Associate's proven gross negligence, willful misconduct, or material breach of this BAA. Covered Entity acknowledges that it maintains sole control over data entered into the ClicData platform, including the presence of any PHI, access configurations, user permissions, and data security practices on its end.

Business Associate shall not be liable for any costs, penalties, or damages arising from the Covered Entity's failure to appropriately secure PHI, misconfigure access controls, or misuse the platform, nor for any breach arising from data that Business Associate has not explicitly accessed, processed, or maintained.

Business Associate's obligation to indemnify Covered Entity shall be limited to actual damages directly caused by its proven gross negligence or willful misconduct and shall exclude any consequential, indirect, punitive, or exemplary damages. In no event shall the

total aggregate liability of Business Associate under this BAA exceed the total fees paid by Covered Entity to Business Associate in the twelve (12) months preceding the event giving rise to the claim.

15. Interpretation.

Any ambiguity in this BAA shall be resolved to permit compliance with HIPAA.

16. Third Party Beneficiaries.

Except for Covered Entity, no third party may rely on the terms, conditions, rights, remedies or obligations hereunder.

17. Applicable Law.

This BAA and its validity, construction and performance shall be governed in all respects by the laws of the State of Delaware, without applicable of conflicts of laws.

BUSINESS ASSOCIATE	**COVERED ENTITY CORPORATION**
ClicData	_____
Name: Telmo Silva	Name: _____
Title: CEO	Title: _____
Date: _____	Date: _____