BUSINESS ASSOCIATE AGREEMENT

This Agreement is entered into by and between:

_____

Your Name
(Hereafter referred to as the **"Healthcare Provider")**

And

Hiltz & Associates
(Hereafter referred to as the "**Business Associate**")

This Agreement ("Agreement") is entered into by and between **the Healthcare Provider** and **the Business Associate** identified above to set forth the terms and conditions under which "individually identifiable health information" ("**Protected Health Information**"), created, received, maintained or transmitted by **the Business Associate** on behalf of **the Healthcare Provider** may be used or disclosed.

For purposes of this Agreement, **Protected Health Information** includes any information that the Business Associate receives from or generates for **the Healthcare Provider**, that identifies the individual, or could be used with other available information to identify the individual, and that concerns the individual's health condition or health care, including payment for health care. The parties desire to enter into this Agreement to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), and the regulations promulgated thereunder, in particular the security and privacy regulations, 45 CFR Parts 160 and 164 and Regulations enacted thereunder, created, received, maintained or transmitted by **the Business Associate** on behalf of **the Healthcare Provider** may be used or disclosed.

This Agreement shall commence on June 1, 2023 and the obligations herein shall continue in effect so long as **the Business Associate** uses, discloses, creates or otherwise possesses any **Protected Health Information** created or received on behalf of **the Healthcare Provider** and until all **Protected Health Information** created or received by **the Business Associate** on behalf of **the Healthcare Provider** is destroyed or returned to **the Healthcare Provider** pursuant to Paragraph 16 herein, unless earlier terminated pursuant to Paragraph 15 herein.

For good and valuable consideration, the receipt of which is hereby acknowledged, the parties agree as follows:

1. **The Healthcare Provider** and **the Business Associate** hereby agree that **the Business Associate** shall be permitted to use and/or disclose **Protected Health Information** created or received on behalf of **the Healthcare Provider** for the following purposes:
    a. Investigating possible fraud and or embezzlement affecting **The Healthcare Provider**.
    b. Investigating and/or correcting inaccuracies in the financial and/or health information maintained on the patients of **the Healthcare Provider**.

It is to be understood by all parties that the permitted uses and disclosures must be within the scope of and necessary to achieve, the obligations and responsibilities of **the Business Associate** in performing on behalf of, or providing services to, **the Health Care Provider**. **The Business Associate** agrees to make uses and disclosures and requests for **Protected Health Information** that are consistent with **the Healthcare Provider's** minimum necessary policies and procedures.

2. **The Business Associate** may only use and disclose **Protected Health Information** created or received on behalf of **the Healthcare Provider** to carry out the specific responsibilities outlined herein, or to comply with legal responsibilities, provided that any disclosure is:
    a. Required by law, or
    b. **The Business Associate** obtains reasonable assurances from the person to whom the **Protected Health Information** is disclosed that
        i. The **Protected Health Information** will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
        ii. **The Business Associate** will be notified of any instances of which the person is aware, in which the confidentiality of the information is breached.
3. **The Business Associate** hereby agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement.
4. **The Business Associate** also agrees to comply with State and Federal laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and regulations thereunder, and all other applicable law.
5. **The Business Associate** further agrees not to use or disclose **Protected Health Information** except as expressly permitted by this Agreement, required by law, or for the purpose of managing **the Business Associate**'s own internal business processes.
6. **The Business Associate** shall not disclose **Protected Health Information** to any member of its workforce unless **the Business Associate** has advised such person of **the Business Associate**'s privacy and security obligations and policies under this Agreement, including the consequences for violation of such obligations. **The Business Associate** shall take appropriate action against any member of its workforce who uses or discloses **Protected Health Information** in violations of this Agreement and applicable law.
7. **The Business Associate** shall not disclose **Protected Health Information** created, received, maintained or transmitted by **the Business Associate** on behalf of **the Healthcare Provider** to a person, including any agent or subcontractor of **the Business Associate** but not including a member of **the Business Associate**'s own workforce, and, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, unless **the Business Associate** obtains

reasonable assurances that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of **the Business Associate** agree to the same restrictions, conditions, and requirements that apply to **the Business Associate** with respect to such information.

8. **The Business Associate** agrees to use appropriate safeguards, including implementation of the requirements of the HIPAA Security Rule, to prevent use or disclosure of **Protected Health Information** not permitted by this Agreement or applicable law.
9. To satisfy **the Healthcare Provider**'s obligations under and in accordance with 45 CFR 164.528, **the Business Associate** agrees to maintain a designated record set of all disclosures of **Protected Health Information**, including disclosures not made for the purposes of this Agreement. Such record shall include the date of the disclosure, the name and, if known, the address of the recipient of the **Protected Health Information**, the name of the individual who is the subject of the **Protected Health Information**, a brief description of the **Protected Health Information** disclosed, and the purpose of the disclosure. **The Business Associate** shall make such record available to an individual who is the subject of such information, or **the Healthcare Provider**, within ten (10) working days of a request.
10. As required by the Breach Notification Rule of the HITECH Act, **The Business Associate** will notify **the Healthcare Provider** as soon as it is aware of any use or disclosure of **Protected Health Information** not provided for by this Agreement by **the Business Associate** or its workforce or subcontractors or other parties, including breaches of unsecured **Protected Health Information** as required by 45 CFR 164.410, and any security incident of which it becomes aware.
11. **The Business Associate** agrees to make its internal practices, books, and records relating to the use and disclosure of **Protected Health Information** received from **the Healthcare Provider,** or created or received by **the Business Associate** on behalf of **the Healthcare Provider**, available to the Secretary of the United States Department of Health and Human Services or any other authorized regulatory agency, for purposes of determining the **Healthcare Provider**'s compliance with HIPAA.
12. In accordance with 45 CFR 164.524, within thirty (30) days of a written request by **the Healthcare Provider**, **the Business Associate** shall allow a person who is the subject of **Protected Health Information**, such person's legal representative, or **the Healthcare Provider** to have access to and to copy such person's **Protected Health Information** in the format requested by such person, legal representative, or practitioner unless it is not readily producible in such format, in which case it shall be produced in standard hard copy format.
13. In accordance with 45 CFR 164.526, **The Business Associate** agrees to make available for amendment, and amend, pursuant to a request by **the Healthcare Provider**, **Protected Health Information** maintained and created or received by **the Business Associate**, on behalf of **the Healthcare Provider**. **The Business Associate** further agrees to complete such amendment within thirty (30) days of a written request by **The Healthcare Provider** and to make such amendment as directed by **the Healthcare Provider** as necessary to satisfy **the Healthcare Provider**'s obligations under 45 CFR 164.126.
14. In the event **the Business Associate** fails to perform the obligations under this Agreement, **the Healthcare Provider** may, at its option:

a. Require **the Business Associate** to submit a plan of compliance, including monitoring by **the Healthcare Provider** and reporting by **the Business Associate**, as **the Healthcare Provider,** in its sole discretion, determines necessary to maintain compliance with this Agreement and applicable law. Such plan shall be incorporated into this Agreement by amendment hereto: and

b. Require **the Business Associate** to mitigate any loss occasioned by the unauthorized disclosure or use of **Protected Health Information**.

c. Immediately discontinue providing **Protected Health Information** to **the Business Associate** with or without written notice to **the Business Associate.**

15. **The Healthcare Provider** may immediately terminate this Agreement and related agreements if **the Healthcare Provider** determines that **the Business Associate** has breached a material term of this Agreement. Alternatively, **the Healthcare Provider** may choose to
    a. Provide **the Business Associate** with ten (10) days written notice of the existence of an alleged material breach; and
    b. Afford **the Business Associate** an opportunity to cure said alleged material breach to the satisfaction of **the Healthcare Provider** within (10) days. **The Business Associate's** failure to cure shall be grounds for immediate termination of this agreement. **The Healthcare Provider's** remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.
16. Upon termination of this Agreement, except where information is required to support possible court testimony on the part of **the Business Associate**, an employee of **the Business Associate** or a subcontractor to **the Business Associate, the Business Associate** shall return or destroy all **Protected Health Information** received from **the Healthcare Provider**, or created or received by **the Business Associate** on behalf of **the Healthcare Provider** and that **the Business Associate** maintains in any form, and shall retain no copies of such information. If the parties mutually agree that return or destruction of **Protected Health Information** is not feasible, **the Business Associate** shall continue to maintain the security and privacy of such **Protected Health Information** in a manner consistent with the obligations of this Agreement and as required by applicable law, and shall limit further use of the information to those purposes that make the return or destruction of the information infeasible. The duties hereunder to maintain the security and privacy of **Protected Health Information** shall survive the termination of this Agreement.
17. Any destruction of **Protected Health Information** that is conducted will be carried out in accordance with **NIST SP 800-88, Guidelines for Media Sanitization** (for electronic media) and destruction of paper records will be carried out by shredding or otherwise rendering the paper records unreadable.
18. The Business Associate will maintain a Certificate of Destruction for any electronic or paper records destroyed pursuant to this agreement.
19. **The Healthcare Provider** may amend this Agreement by providing ten (10) days prior written notice to **the Business Associate** to maintain compliance with applicable State or Federal law. Such amendment shall be binding upon **the Business Associate** at the end of the ten (10) day period and shall not require the consent of **the Business Associate. The Business Associate** may elect to discontinue the Agreement within the ten (10) day period, but **the Business Associate**

duties hereunder to maintain the security and privacy of **Protected Health Information** shall survive such discontinuance. **The Healthcare Provider** and **the Business Associate** may otherwise amend this Agreement by mutual written agreement.

20. **The Business Associate** shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless **the Healthcare Provider** and his/her respective employees, directors, and agents ("Indemnitiees") from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorneys' fees, including at trial and on appeal) asserted or imposed against any Indemnitiees arising out of the acts or omissions of **the Business Associate** or any of **the Business Associate's** employees, directors, or agents related to the performance or nonperformance of this Agreement.
21. The following terms used in this Agreement have the same meaning ascribed to those terms in the HIPAA Rules: breach, designated record set, disclosure, individual, minimum necessary, Protected Health Information, required by law, Secretary, security incident, subcontractor, unsecured Protected Health Information, and use. The following specific definitions shall be used:
    a. **Business Associate**. "**Business Associate**" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean Hiltz & Associates Inc.
    b. **HIPAA Rules**. "**HIPAA Rules**" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
22. To the extent that any provision of this Agreement conflicts with the HIPAA Rules, then the HIPAA Rules shall control and this Agreement shall be deemed amended in such respect as is necessary to cause it to comply with the HIPAA Rules.

Hiltz & Associates
The Business Associate

William (Bill) Hiltz BSc MBA CET
CEO and Founder **June 1, 2023**

Office: 201-503-3742 | Cell: 201-467-4987
Fax: 855-440-8624 | Email: william@hiltzandassociates.com
Company: https://hiltzandassociates.com