BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is made effective as of **[Date - same as service agreement]**, by and between **Expert AI**, (hereinafter referred to as "Business Associate"), and **[Client Company Name/Individual Name]**, (hereinafter referred to as "Covered Entity").

RECITALS

WHEREAS, Covered Entity is a healthcare provider subject to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and their implementing regulations (collectively, "HIPAA")[1];

WHEREAS, Covered Entity engages Business Associate to provide AI-powered medical transcription and documentation services as described in the Service Agreement dated **[Date of Service Agreement]** (the "Service Agreement"), which may require Business Associate to create, receive, maintain, or transmit Protected Health Information ("PHI") on behalf of Covered Entity[2];

WHEREAS, the parties intend to comply with the requirements of HIPAA, including but not limited to 45 CFR Part 164, Subpart C and E, and Subtitle D of the HITECH Act, regarding the use and disclosure of PHI[3];

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the parties agree as follows:

1. Definitions

Unless otherwise specified, capitalized terms used in this BAA shall have the same meaning as those terms in HIPAA[4].

- **"Breach"** shall have the meaning given to it in 45 CFR § 164.402[5].
- **"PHI"** (Protected Health Information) shall have the meaning given to it in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity[6].
- **"Security Incident"** shall have the meaning given to it in 45 CFR § 164.304[7].
- **"Service Agreement"** means the agreement between Covered Entity and Business Associate for the provision of services, to which this BAA is incorporated or attached[8].

2. Permitted Uses and Disclosures of PHI by Business Associate

2.1 General Rule: Business Associate may use or disclose PHI only as necessary to perform the services set forth in the Service Agreement, as permitted or required by this BAA, or as required by law[9].

2.2 Specific Permitted Uses and Disclosures:

- a. For Covered Entity's Operations:

Business Associate may use and disclose PHI for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses and disclosures are permitted by law[10].

- b. Data Aggregation:

Business Associate may use PHI to provide data aggregation services relating to the health care operations of the Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B)[11].

- c. De-identification:

Business Associate may de-identify PHI in accordance with 45 CFR § 164.514(b) and may use and disclose such de-identified information for any purpose permitted by law, including for the purpose of improving its services and training its artificial intelligence models[12].

- d. Minimum Necessary:

Business Associate agrees to use, disclose, and request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request, consistent with 45 CFR § 164.502(b) and § 164.514(d)[13].

3. Obligations of Business Associate

Business Associate agrees to:

3.1 Not Use or Disclose PHI: Not use or disclose PHI other than as permitted or required by this BAA or as required by law[14].

3.2 Safeguards: Implement and maintain appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, in accordance with the HIPAA Security Rule (45 CFR Part 164, Subpart C)[15]. Such safeguards shall include, at a minimum:

- **a. Encryption:** The encryption of all electronic PHI while in transit and at rest.
- **b. Access Controls:** The implementation of robust, role-based access controls to ensure only authorized personnel have access to PHI on a need-to-know basis.

- **c. Audit Trails:** The maintenance of audit logs and trails that record and examine activity in information systems that contain or use electronic PHI.

3.3 Reporting of Security Incidents and Breaches:

- **a.** Report to Covered Entity any Security Incident of which it becomes aware without unreasonable delay, and in no case later than five (5) business days of discovery[16].
- **b.** Report to Covered Entity any suspected or actual Breach of unsecured PHI discovered by Business Associate without unreasonable delay, and in no case later than five (5) business days of discovery[17]. Such notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed[18]. Business Associate shall cooperate with Covered Entity in the investigation of any such Breach[19].

3.4 Mitigation: 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 BAA[20].

3.5 Subcontractors: Ensure that any agents or subcontractors to whom Business Associate provides PHI agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI[21].

3.6 Access to PHI: Make available PHI in a Designated Record Set to the Covered Entity or, as directed, to an individual to satisfy the individual's right of access under 45 CFR § 164.524, within ten (10) business days of Covered Entity's request[22].

3.7 Amendments to PHI: Make available PHI for amendment and incorporate any amendments as directed by Covered Entity in accordance with 45 CFR § 164.526, within ten (10) business days of Covered Entity's request[23].

3.8 Accounting of Disclosures: Maintain and make available the information required to provide an accounting of disclosures of PHI as required by 45 CFR § 164.528, within ten (10) business days of Covered Entity's request[24].

3.9 Data Retention: Retain PHI for a period of up to seven (7) years from the date of creation or last use, as necessary to provide the Services or as required by applicable law, after which the PHI will be disposed of in a secure and confidential manner.

3.10 Compliance with HHS: Make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of HHS for purposes of determining compliance with HIPAA[25].

4. Obligations of Covered Entity

4.1 Notice of Privacy Practices: Covered Entity shall notify Business Associate of any limitation in its Notice of Privacy Practices that may affect Business Associate's use or disclosure of PHI[26].

4.2 Changes in Permissions: Covered Entity shall notify Business Associate of any changes in, or revocation of, 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[27].

4.3 Restrictions: Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR § 164.522[28].

4.4 Permitted Uses and Disclosures: Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity[29].

5. Term and Termination

5.1 Term: This BAA shall become effective on the Effective Date and shall terminate when all PHI is destroyed or returned to Covered Entity as provided in Section 5.3[30].

5.2 Termination for Cause: Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach within a reasonable time specified by Covered Entity[31]. If the breach is not cured within the specified time, Covered Entity shall terminate this BAA and the Service Agreement[32]. If termination is not feasible, Covered Entity shall report the violation to the Secretary of HHS[33].

5.3 Effect of Termination:

- **a.** Upon termination of this BAA for any reason, Business Associate shall return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form[34]. Business Associate shall retain no copies of such PHI[35].
- **b.** If return or destruction of PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible[36].

6. Miscellaneous

6.1 Survival: The respective rights and obligations of Business Associate under Section 5.3 of this BAA shall survive the termination of this BAA[37].

6.2 Indemnification: Business Associate agrees to indemnify, defend, and hold harmless Covered Entity and its officers, directors, employees, and agents from and against any and all

claims, losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising from or related to any negligent or wrongful act or omission of Business Associate or its subcontractors in violation of its obligations under this BAA.

6.3 Insurance: Business Associate shall maintain, at its sole expense, a policy of cybersecurity liability insurance with limits of not less than $1,000,000 per claim and $3,000,000 in the annual aggregate. Business Associate shall provide a certificate of insurance to Covered Entity upon request.

6.4 No Third-Party Beneficiaries: Nothing in this BAA is intended to confer any rights or remedies upon any person other than the parties and their respective successors and assigns[38].

6.5 Entire Agreement: This BAA, together with the Service Agreement, constitutes the entire agreement between the parties with respect to its subject matter[39].

6.6 Amendment: The parties agree to amend this BAA as necessary to comply with the requirements of HIPAA[40].

6.7 Interpretation: Any ambiguity in this BAA shall be interpreted to permit compliance with HIPAA[41].

6.8 Governing Law: This BAA shall be governed by and construed in accordance with the laws of the State of **Michigan**, without regard to its conflict of laws principles[42].

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the date first above written[43].

Expert AI