BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made and entered into as of [Effective Date], by and between Better Health Together, a Washington nonprofit corporation ("Covered Entity"), and [Business Associate Name], ("Business Associate"). This Agreement is established to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the implementing regulations at *45 C.F.R. Parts 160* and *164*. It ensures that Business Associate appropriately safeguards Protected Health Information (PHI) received from, or created or maintained on behalf of, Covered Entity.

1. **Purpose**
   - Purpose. The purpose of this Agreement is to ensure compliance with the HIPAA Privacy Rule (*45 C.F.R. Part 164, Subpart E*), the HIPAA Security Rule (*45 C.F.R. Part 164, Subpart C*), and the Breach Notification Rule (*45 C.F.R. Part 164, Subpart D*). This Agreement establishes Business Associate's obligations regarding the protection, use, and disclosure of PHI, including electronic PHI (ePHI). Business Associate agrees to implement appropriate security safeguards to protect PHI from unauthorized access, use, or disclosure and to notify Covered Entity of any breaches or security incidents within the timeframe specified in this Agreement.
   - Effect. This Agreement supersedes any prior business associate agreement between the parties, and those portions of any agreement between the parties that involve the disclosure of PHI by Covered Entity to Business Associate. To the extent any conflict or inconsistency between this Agreement and the terms and conditions of any other agreement exists, the terms of this Agreement will control.
   - Amendment. Covered Entity may, without Business Associate's consent, amend this Agreement to maintain consistency and/or compliance with any state or federal law, policy, directive, regulation, or government sponsored program requirement, upon forty-five (45) business days' notice to the Business Associate unless a shorter timeframe is necessary for compliance. Covered Entity may otherwise materially amend this Agreement only after forty-five (45) business days prior written notice to the Business Associate and only if mutually agreed to by the parties as evidenced by the amendment being executed by each party hereto. If the parties fail to execute a mutually agreeable amendment within forty-five (45) days of the Business Associate's receipt of Covered Entity's written notice to amend this Agreement, Covered Entity shall have the right to immediately terminate this Agreement and any other agreement(s) between the Parties which may require the Business Associate's use or disclosure of PHI in performance of services described in such agreement(s) on behalf of Covered Entity.

2. **Definitions**
   - Protected Health Information (PHI): Any individually identifiable health information transmitted or maintained in any form or medium, including electronic, paper, or oral formats, as defined in *45 C.F.R. § 160.103*.
   - Electronic Protected Health Information (ePHI): A subset of PHI that is transmitted or maintained in electronic form, as defined in *45 C.F.R. § 160.103*.
   - Security Incident: An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, as defined in *45 C.F.R. § 164.304*.
   - Breach: The acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA, which compromises the security or privacy of the PHI, as defined in *45 C.F.R. § 164.402*.
   - HIPAA Rules: Collectively refers to the Privacy Rule, Security Rule, and Breach Notification Rule under *45 C.F.R. Parts 160* and *164*.

3. Obligations of Business Associate

3.1. Use and Disclosure of PHI

(a) Permitted Uses and Disclosures

Business Associate may use or disclose PHI only as necessary to perform the services outlined in its agreement with Covered Entity, or as required by law, in accordance with 45 C.F.R. § 164.502(a). Business Associate may not use or disclose PHI in any manner that would violate HIPAA if conducted by Covered Entity, except as specifically permitted in this Agreement.

- Use for Service Performance – Business Associate may use PHI as necessary to perform its obligations under the Underlying Services Agreement with Covered Entity.
- Use for Proper Management and Administration – Business Associate may use PHI for its own internal management and administrative purposes, or for legal obligations, provided that such use is permitted under *45 C.F.R. § 164.504(e)(4).*
- Disclosure for Legal Requirements – Business Associate may disclose PHI when required by law, provided that it notifies Covered Entity of such disclosures prior to release, unless prohibited by law.

(b) Prohibited Uses and Disclosures

Unless explicitly authorized by Covered Entity or required by law, Business Associate shall not:

- Sell PHI or use PHI for marketing purposes without obtaining individual authorization, as required by *45 C.F.R. § 164.508(a)(3)* & *§ 164.502(a)(5)(ii).*
- Use PHI for its own commercial purposes, including data analytics or research, unless specifically permitted in writing by Covered Entity.
- Disclose PHI to third parties who do not have a HIPAA-compliant agreement with Business Associate for permitted uses under this Agreement.

(c) Special Categories of PHI

Business Associate acknowledges that certain types of PHI are subject to additional legal protections under HIPAA, *42 C.F.R. Part 2* (for Substance Use Disorder records), and applicable state laws. Business Associate shall comply with the following requirements when handling these categories:

(1) Reproductive Health Information:

PHI related to reproductive health services (including but not limited to contraceptive care, abortion services, fertility treatments, and gender-affirming care) is subject to additional legal protections under various state laws and federal regulations. Business Associate:

- Shall not disclose reproductive health PHI unless required by law or with explicit patient authorization under *45 C.F.R. § 164.508*.
- Must notify Covered Entity before any disclosure, unless legally prohibited.
- Shall implement additional safeguards to prevent unauthorized access or disclosures.

(2) Part 2 Substance Use Disorder (SUD) Records:

If Business Associate receives, maintains, or transmits PHI that qualifies as Substance Use Disorder (SUD) treatment records, it shall comply with *42 C.F.R. Part 2*, which provides stricter protections than HIPAA. Business Associate shall:

- Not use or disclose SUD records without explicit patient consent, except as permitted by *42 C.F.R. § 2.33*.
- Ensure all disclosures include the required Part 2 redisclosure notice, stating that such records may not be re-disclosed without specific authorization.
- Limit access to Part 2 records to only those employees with a legitimate need to know.

(3) Psychotherapy Notes:

Psychotherapy notes, as defined under *45 C.F.R. § 164.501*, receive heightened protection under HIPAA. Business Associate shall:

- Not use or disclose psychotherapy notes without explicit written patient authorization, except in limited circumstances (e.g., legal defense of the provider, per *45 C.F.R. § 164.508(a)(2)).*
- Maintain psychotherapy notes separately from the rest of a patient's medical record.
- Exclude psychotherapy notes from general access and disclosure requests, unless required by law.

(4) Redisclosure Prohibitions:
Any PHI classified as Substance Use Disorder Records *(42 C.F.R. Part 2),* Reproductive Health Information, or Psychotherapy Notes shall not be re-disclosed without explicit patient consent, unless required by law. Business Associate shall ensure all disclosures include appropriate legal disclaimers.

(d) Minimum Necessary Standard:
Business Associate shall adhere to the minimum necessary standard as required under *45 C.F.R. § 164.502(b).* Business Associate shall make reasonable efforts to limit PHI use, disclosure, and requests to the minimum amount necessary to accomplish the intended purpose.

(e) Subcontractors and Third-Party Disclosures:
Business Associate may disclose PHI to subcontractors only if:
- The subcontractor has executed a HIPAA-compliant Business Associate Agreement (BAA) with Business Associate, in accordance with *45 C.F.R. § 164.502(e)(1)(ii).*
- The subcontractor agrees to implement appropriate administrative, physical, and technical safeguards to protect PHI.
- Business Associate actively monitors subcontractor compliance and promptly addresses any security concerns.

If Business Associate discovers that a subcontractor has violated the terms of its BAA, it shall:
- Take immediate corrective action to remediate the issue.
- Notify Covered Entity promptly but no more than five (5) days of discovering the violation.
- Terminate the relationship if the subcontractor fails to implement adequate safeguards.

3.2. Safeguards & Cybersecurity Measures

Business Associate shall implement appropriate administrative, physical, and technical safeguards, in compliance with *45 C.F.R. §§ 164.308*, *164.310*, and *164.312*, to ensure the confidentiality, integrity, and availability of PHI. Business Associate shall establish measures to identify, assess, and mitigate cybersecurity risks associated with its products and services, including implementing an incident response protocol to detect, respond to, and recover from cybersecurity threats.

(a) Encryption & Secure Data Handling:
Business Associate shall ensure that all electronic PHI (ePHI) is encrypted at rest and in transit using industry standards. PHI shall not be transmitted via unencrypted email, unsecured FTP, or other non-compliant methods.

3.3. Security Incident and Breach Notification

(a) Reporting of Security Incidents and Breaches:
Business Associate shall report to Covered Entity any Security Incident or Breach of Unsecured PHI as required by *45 C.F.R. § 164.410*. Business Associate shall notify Covered Entity without unreasonable delay and in no event later than thirty (30) days from the date the breach is discovered. A breach shall be deemed discovered on the first day it is known to Business Associate or should have been known through the exercise of reasonable diligence.

(b) Content of Notification:

The notification to Covered Entity shall include, to the extent known at the time of reporting:

- A description of the breach, including the date of occurrence and the date of discovery.
- The types of PHI involved, including whether information such as names, addresses, dates of birth, Social Security numbers, medical record numbers, health insurance information, or financial data were compromised.
- The number of individuals affected, if known.
- The scope and nature of the unauthorized access, use, or disclosure, including whether the PHI was acquired, accessed, or viewed without authorization.
- Corrective actions taken or planned to mitigate harm and prevent further breaches.
- Steps affected individuals should take to protect themselves from potential harm, if applicable.
- The name and contact information of a Business Associate representative designated to respond to inquiries regarding the breach.

(c) Special Considerations for Breaches Involving Sensitive PHI

- If a breach involves reproductive health information, Part 2 SUD records, or psychotherapy notes, Business Associate shall take additional measures to mitigate harm, including:
- Providing enhanced breach notification that specifies whether sensitive PHI was compromised.
- Offering additional support, such as identity theft protection or counseling resources, if required by law.
- Coordinating with Covered Entity on public disclosures or regulatory reporting to minimize harm.

(d) Ongoing Updates and Final Report:

If all information is not immediately available, Business Associate shall provide an initial notification with the available details and submit regular updates as additional information becomes available. A final written report summarizing the breach, mitigation efforts, and corrective actions taken shall be submitted to Covered Entity as soon as possible but no later than thirty (30) days after initial notification.

(e) Responsibility for Breach Notification:

Business Associate shall cooperate fully with Covered Entity to comply with breach notification obligations under *45 C.F.R. §§ 164.400-414.*

3.4. Subcontractors

(a) Requirement to Bind Subcontractors to HIPAA Obligations:

If Business Associate engages any subcontractor to perform functions, activities, or services involving the creation, receipt, maintenance, or transmission of PHI on behalf of Business Associate, Business Associate shall ensure that such subcontractor agrees in writing to comply with HIPAA regulations and the same privacy, security, and breach notification obligations imposed on Business Associate under this Agreement, in accordance with *45 C.F.R. § 164.502(e)(1)(ii)* and *45 C.F.R. § 164.308(b)(2).*

(b) Due Diligence and Risk Assessment of Subcontractors:

Business Associate shall perform appropriate due diligence on all subcontractors handling PHI to ensure they implement and maintain reasonable and appropriate administrative, physical, and technical safeguards to protect PHI in compliance with *45 C.F.R. § 164.308, 164.310,* and *164.312*. Business Associate shall document its risk assessment and ensure that subcontractors have policies and procedures to mitigate risks related to cybersecurity threats, unauthorized disclosures, and breaches.

(c) Monitoring and Compliance of Subcontractors:

Business Associate shall establish processes to monitor subcontractors for compliance with HIPAA and this Agreement. If Business Associate becomes aware of a subcontractor's failure to comply with these obligations, Business Associate shall take immediate steps to remediate the issue, including requiring corrective action or terminating the subcontractor's access to PHI, if necessary.

(d) AI & Third-Party Processing Restrictions:

Business Associate shall not use automated decision-making, artificial intelligence, or machine learning algorithms to process PHI without prior written approval from Covered Entity. Business Associate shall also disclose any offshore data processing arrangements before engaging subcontractors outside the United States.

3.5. Access, Amendment, and Accounting of PHI

(a) Access to PHI by Individuals:

In accordance with *45 C.F.R. § 164.524*, Business Associate shall make PHI available to Covered Entity upon request, to allow individuals to access their PHI as required under HIPAA. Business Associate shall provide access to PHI in a designated record set within ten (10) days of receiving a written request from Covered Entity. If Business Associate maintains PHI electronically, it must provide such PHI in an electronic format if requested by the individual, unless it is not technically feasible. Business Associate shall not deny access to PHI except as permitted by HIPAA or as directed by Covered Entity.

(b) Amendment of PHI:

In accordance with *45 C.F.R. § 164.526*, if an individual requests an amendment to their PHI and Covered Entity determines that the amendment is appropriate, Business Associate shall make the requested amendment(s) within fifteen (15) days of receiving a request from Covered Entity. If Business Associate does not agree with the requested amendment, it must provide a written statement explaining its reasons and follow Covered Entity's instructions regarding the handling of the disputed information. Business Associate shall incorporate any amendments, corrections, or statements of disagreement into the designated record set as required by HIPAA.

(c) Accounting of Disclosures:

Pursuant to *45 C.F.R. § 164.528*, Business Associate shall document and maintain a record of all disclosures of PHI made outside the scope of routine treatment, payment, or healthcare operations. Business Associate shall provide Covered Entity with an accounting of such disclosures within twenty (20) days of a request, including the following details:

- Date of disclosure.
- Name and address of the recipient.
- Description of the PHI disclosed.
- Purpose of the disclosure, including the applicable legal basis.

For disclosures made using an electronic health record (EHR), Business Associate shall account for disclosures for at least three (3) years prior to the request, in accordance with the HITECH Act. If Business Associate receives an individual's request for an accounting of disclosures directly, it shall forward the request to Covered Entity within five (5) days and shall not respond directly unless authorized by Covered Entity.

(d) Special Considerations for Sensitive PHI:

Business Associate shall process requests for access, amendment, and accounting of disclosures related to reproductive health information, psychotherapy notes, and Part 2 SUD records in accordance with the applicable heightened privacy standards.

- Psychotherapy Notes – Business Associate shall not provide access to psychotherapy notes without the explicit written authorization of the individual, unless permitted by *45 C.F.R. § 164.524(a)(1)(ii).*

- Substance Use Disorder Records – Business Associate shall not disclose SUD records without the patient's written consent, except under a Part 2-permitted exception *(42 C.F.R. § 2.33).*

- Reproductive Health Information – Business Associate shall implement safeguards to prevent unauthorized disclosure, including limiting access to personnel with a legitimate need-to-know.

(e) Documentation and Retention of Records:
Business Associate shall maintain documentation related to access requests, amendments, and accounting of disclosures for a minimum period of six (6) years, as required under *45 C.F.R. § 164.530(j).*

(f) Compliance with the 21st Century Cures Act:
Business Associate shall not engage in information blocking, as defined in *45 C.F.R. Part 171*, and shall provide PHI in the format requested (electronic or paper) without unreasonable delay. If Business Associate cannot fulfill a request, it must document the reason and notify Covered Entity.

4. Obligations of Covered Entity

(a) Minimum Necessary Standard:
Covered Entity shall disclose to Business Associate only the minimum necessary PHI required for Business Associate to perform its services, as required under *45 C.F.R. § 164.502(b)*. Covered Entity shall review and implement policies to ensure PHI disclosures are limited to the minimum information necessary to accomplish the intended purpose.

(b) Authorization and Consent Requirements:
Covered Entity shall be responsible for obtaining any necessary authorizations, consents, or legal permissions required under *45 C.F.R. § 164.508* before instructing Business Associate to use or disclose PHI in a manner beyond the routine uses permitted under this Agreement. Covered Entity shall provide Business Associate with clear documentation regarding any limitations or restrictions imposed on PHI.

(c) Notification of Changes in HIPAA Policies or PHI Restrictions:
Covered Entity shall notify Business Associate in writing of any changes in its privacy practices, restrictions on PHI, or security requirements that may impact Business Associate's obligations under this Agreement. Business Associate shall have a reasonable time to implement such changes and ensure compliance.

(d) Cooperation in Incident Response and Compliance Audits:
In the event of a security incident, data breach, or government investigation, Covered Entity shall cooperate with Business Associate to respond to regulatory inquiries, audits, or legal proceedings. Covered Entity shall provide Business Associate with relevant information or documentation needed to comply with HIPAA's breach notification and enforcement requirements under *45 C.F.R. Part 160, Subparts C and D*.

(e) Right to Audit and Inspect Business Associate:
Covered Entity reserves the right to audit, inspect, or request compliance documentation from Business Associate upon reasonable notice to ensure Business Associate is meeting its obligations under HIPAA and this Agreement. Business Associate shall provide all requested documentation, reports, and policies necessary to demonstrate compliance.

5. Term & Termination

(a) Term

This Agreement shall become effective on Effective Date and shall remain in effect until terminated by either party or upon the expiration or termination of the underlying service agreement between Covered Entity and Business Associate, unless otherwise specified herein.

(b) Termination for Cause

Covered Entity may terminate this Agreement upon five (5) days' written notice if it determines, in its sole discretion, that Business Associate has materially violated a term of this Agreement, has failed to comply with the applicable provisions of HIPAA, the HITECH Act, or 42 C.F.R. Part 2 (if applicable) or if Business Associate has defaulted (beyond any applicable notice and cure period therein) under any service agreement between the parties involving the use and disclosure of PHI.

(c) Effect of Termination

Upon termination of this Agreement for any reason, Business Associate shall, at the direction of Covered Entity:

- Return or Destroy PHI – Business Associate shall return or securely destroy all PHI received, created, or maintained on behalf of Covered Entity in compliance with *45 C.F.R. § 164.504(e)(2)(ii)(J).*
- Retention Exception – If Business Associate determines that returning or destroying PHI is not feasible, Business Associate shall provide Covered Entity with a written explanation of the reasons for retention and extend all protections under this Agreement to the retained PHI for as long as it is maintained.
- Subcontractor Compliance – Business Associate shall ensure that any subcontractors or agents who received PHI also return or destroy such PHI, unless infeasible, in which case the same protections shall apply.
- Ongoing Confidentiality Obligations – Even after termination, Business Associate shall not use or disclose PHI except as required by law or for purposes agreed upon in writing with Covered Entity.

(d) Survival

The rights and obligations under this Term and Termination section, as well as any provisions related to PHI confidentiality, security, indemnification, and breach notification, shall survive the termination of this Agreement.

(f) Retention of Sensitive PHI Upon Termination

If Business Associate cannot return or destroy reproductive health records, Part 2 SUD records, or psychotherapy notes upon termination of this Agreement, it shall:

- Maintain the records under heightened security in compliance with HIPAA and *42 C.F.R. § 2.19*.
- Ensure access is strictly limited to personnel with a legal need-to-know.
- Extend the protections of this Agreement indefinitely for retained sensitive PHI.

6. Indemnification & Liability

Business Associate shall indemnify, defend, and hold harmless the Covered Entity, and Covered Entity's affiliates ("Indemnified Parties"), from and against any and all losses, expense, damage, or injury (including, without limitation, all costs and reasonable attorney's fees) that the Indemnified Parties may sustain as a result of, or arising out of: (a) a breach of this Agreement by Business Associate or its agents or Subcontractors, including but not limited to any unauthorized use, disclosure, or breach of PHI; (b) Business Associate's failure to notify any and all parties required to receive notification of any breach of Unsecured PHI pursuant this Agreement; or (c) any negligence or wrongful acts or omissions by Business Associate or its agents or Subcontractors, including without limitations, failure to perform Business Associate's obligations under this Agreement, the Privacy Rule, the Security Rule, and any default by Business Associate under any service agreement between the parties involving the use and disclosure of PHI. Notwithstanding the

foregoing, nothing in this Section will limit any rights that any of the Indemnified Parties may have to additional remedies under any service agreement between the parties or under applicable law for any acts or omissions of Business Associate or its agents or Subcontractors. Business Associate shall be responsible for all costs associated with breach notification, regulatory fines, and any required mitigation efforts. The terms of this Section will survive the expiration or earlier termination of this Agreement.

7. Miscellaneous

Except as preempted by federal law, this Agreement shall be governed by the laws of the State of Washington, without regard to conflict-of-law principles. The venue will be the jurisdiction where the applicable services were received by Covered Entity. Except as otherwise provided in this Agreement, amendments must be made in writing and signed by both parties. If any provision of this Agreement is found invalid, the remainder shall remain in effect. Business Associate acknowledges it is directly subject to HIPAA enforcement and must comply with all applicable regulatory requirements. Any notices to be given under this Agreement to a party must be made by certified mail with return receipt request or federal express to such party's address listed below their signature to this Agreement. Such notices will be deemed delivered three (3) days after mailed certified with return receipt request or one (1) day after mailed federal express for overnight delivery. Nothing express or implied in this Agreement is intended to confer, nor shall anything in this Agreement confer, upon any person other than the parties hereto and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever. This Agreement shall be interpreted in the following manner: (a) any ambiguity shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules; (b) any inconsistency between the Agreement's provisions and the HIPAA Rules, including all amendments, as interpreted by the HHS, a court, or another regulatory agency with authority over the parties, shall be interpreted according to the interpretation of the HHS, the court, or the regulatory agency; and (c) any provision of this Agreement that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be adhered to as stated in this Agreement. This Agreement will be binding on the successors and permitted assigns of the Covered Entity and the Business Associate; however, this Agreement may not be assigned by Business Associate, in whole or in part, without the written consent Covered Entity, and any attempted assignment in violation of this provision shall be null and void. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
BETTER HEALTH TOGETHER	**ORGANIZATION NAME**
By: _____	By: _____
Alison Poulsen	Signer Name
President	Title
Date: _____	Date: _____
Address:	Address:
PO Box 271	Line 1
Spokane WA 99210	Line 2