Appendix 4 – HIPAA Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into and is in effect as of by and between , on behalf of itself and all present and future affiliates (hereinafter referred to as the "Covered Entity") and the **DIRIGO HEALTH AGENCY**, an independent executive agency of the State of Maine (hereinafter referred to as "Business Associate") (collectively the "Parties").

WHEREAS, the Parties wish to enter into or have entered into an arrangement ("Arrangement") whereby Business Associate will provide certain services to Covered Entity and, in providing those services, Business Associate may have access to Protected Health Information ("PHI")(defined below) and may maintain, transmit and receive Electronic Protected Health Information ("EPHI")(defined below)(PHI and EPHI are collectively referred to herein as PHI or Protected Health Information; EPHI will be used when only EPHI is being referenced);

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of any PHI which shall be disclosed to Business Associate pursuant to the Arrangement, in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated thereunder by the United States Department of Health and Human Services ("HIPAA Regulations") and other applicable laws; and

WHEREAS, as part of the HIPAA Regulations, the Privacy and Security Rule (defined below) requires Business Associate to enter into a contract containing specific provisions intended to preserve the confidentiality and security of PHI obtained by Business Associate in the course of its business relationship with Covered Entity (defined below) prior to any disclosure of the PHI to Business Associate. The specific provisions are set forth in, but not limited to, Title 45, Sections 164.306, 164.308(b), 164.314(a) and (b), 164.502(e) and 164.504(e) of the Code of Federal Regulations and are applicable to this Agreement.

NOW THEREFORE, in consideration of the mutual promises below, and the exchange of PHI pursuant to the terms of this Agreement, the Parties agree as follows:

1.0 DEFINITIONS

As used in this Agreement, the following terms shall have the indicated meaning. Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR Sections 160.103 and 164.501. The definitions below which set forth a reference to the Code of Federal Regulations are defined HIPAA terms, and such definitions are incorporated herein as though set forth in full. A change to the HIPAA Regulations which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

1.1 **Arrangement** means the non-binding Letter of Intent executed between the Parties and, if executed, the definitive agreement between Covered Entity and Business Associate, whereby Business Associate provides or will provide certain services to Covered Entity and, in providing those services, may have access to PHI.

1.2 **Authorization** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.508.

1.3 **Business Associate** shall mean the Dirigo Health Agency. Where the term "business associate" appears without initial capital letters, it shall have the meaning given to such term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.4 **Covered Entity** shall mean ., as defined. It shall also have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.5 **Data Aggregation** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.6 **Designated Record Set** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.7 **Electronic Protected Health Information ("EPHI")** shall have the meaning given to the term Electronic Protected Health Care Information under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.8 **Health Care Operations** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.9 **Individual** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501. It shall also include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

1.10 **Privacy and Security Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information that is codified at 45 CFR parts 160 and 164.

1.11 **Protected Health Information ("PHI")** means any information, whether oral or recorded in any form, or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an

individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual, and shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.12 **Required by Law** shall have the meaning given to the term under the Privacy and Security Rule, including but not limited to, 45 CFR Section 164.501.

1.13 **Security Incident** shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI, or interference with system operations in an information system.

1.14 **Security Standards** shall mean those security standards promulgated or to be promulgated pursuant to HIPAA and other applicable federal or state regulations or statutes.

2.0 Obligations of Business Associate

2.1 **Use and Disclosure of Protected Health Information.** Business Associate may use and disclose PHI only as required to satisfy its obligations under the Arrangement or this Agreement, as permitted herein, or as Required by Law, but shall not otherwise use or disclose any PHI. Business Associate shall not, and shall ensure that its directors, officers, employees, contractors and agents do not, use or disclose PHI in any manner that would constitute a violation of the Privacy and Security Rule if done by the Covered Entity, except that Business Associate may use PHI if necessary (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) to provide Data Aggregation services relating to the Health Care Operations of the Covered Entity. Business Associate further represents that, to the extent it requests Covered Entity to disclose PHI to Business Associate, such request will only be for the minimum PHI necessary for the accomplishment of Business Associate's purpose.

2.2 **Safeguards Against Misuse of Information.** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement.

2.3 **Mitigation of Harmful Effects.** Business Associate agrees to 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 Agreement.

2.4 **Reporting of Violations.** Business Associate shall, within thirty (30) days of becoming aware of any use or disclosure of PHI in violation of this Agreement

by Business Associate or any of its officers, directors, employees, contractors or agents, report such use or disclosure to the Covered Entity.

2.5 **Agreements by Third Parties.** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides or transmits PHI received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.6 **Access to Information.** Within ten (10) days of a request by Covered Entity for access to PHI about an Individual contained in a Designated Record Set, Business Associate shall make available to Covered Entity such PHI in order to enable Covered Entity to meet the requirements of 45 CFR Section 164.524. In the event any Individual requests access to his or her PHI directly from Business Associate, it shall within two (2) days forward such request to Covered Entity so that Covered Entity can comply with the request. Business Associate shall not provide direct access to any Individual who requests access to his or her PHI. Any denials of access to the PHI requested shall be the responsibility of Covered Entity.

2.7 **Availability of Protected Health Information for Amendment.** Within thirty (30) days of receipt of a request from Covered Entity for the amendment of an Individual's PHI or a record regarding an individual contained in a Designated Record Set, Business Associate shall provide such information to Covered Entity for amendment and shall incorporate any such amendments in the PHI as required by 45 CFR Section 164.526. Any denials of requested amendments shall be the responsibility of Covered Entity.

2.8 **Accounting of Disclosures.** Within twenty (20) days of making a disclosure of PHI, other than disclosures excepted under 45 CFR Section 164.528(a), Business Associate shall report such disclosure to Covered Entity in writing. At a minimum, Business Associate shall provide the following information for each disclosure: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. In the event that an Individual's request for an accounting is delivered directly to Business Associate, it shall within five (5) days forward such request to the Covered Entity so that Covered Entity can comply with the request. Such information must be maintained by Business Associate and its agents and subcontractors for a period of six (6) years from the date of each disclosure.

2.9 **Safeguarding EPHI.** Business Associate agrees to:

2.9.1 Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and

availability of the EPHI that it creates, receives, maintains or transmits on behalf of the Covered Entity in connection with this Agreement;

2.9.2 Ensure that any agent, including a subcontractor, to whom it provides such EPHI agrees to implement reasonable and appropriate safeguards to protect it; and

2.9.3 Report promptly in writing to the Covered Entity any Security Incident of which it becomes aware.

2.10 **Auditing, Inspections and Enforcement.** Upon reasonable notice, Business Associate agrees to make its internal practices, books and records relating to the use or disclosure of PHI available to Covered Entity and the Secretary of the Department of Health and Human Services, or the Secretary's designee, for purposes of determining Covered Entity's compliance with the Privacy and Security Rule. Business Associate shall provide appropriate training regarding the requirements of this Agreement to any employee accessing, using or disclosing PHI and shall develop and implement a system of sanctions for any employee, agent or subcontractor who violates this Agreement.

2.11 **Indemnification.** Business Associate shall indemnify and hold harmless Covered Entity from and against any and all losses, expense, damage or injury that Covered Entity sustains as a result of, or arising out of a breach of this Agreement by Business Associate or its agents or subcontractors, including but not limited to any unauthorized use or disclosure of PHI.

2.12 **Notice of Request for Data.** Business Associate agrees to notify Covered Entity within five (5) days of Business Associate's receipt of any request, subpoena, or judicial or administrative order to disclose PHI. To the extent the Covered Entity decides to assume responsibility for challenging the validity of such request, subpoena or order, Business Associate agrees to cooperate with Covered Entity in such challenge.

3.0 **Covered Entity's Obligations.**

3.1 **Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of any privacy practices that Covered Entity produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Business Associate shall not distribute its own notice, if any, to Individuals, without the prior written consent of Covered Entity.

3.2 **Revocation of Authorization by Individual.** Covered Entity agrees to inform Business Associate of any change to, or revocation of, an Individual's Authorization to use or disclose PHI to the extent that such change may affect Business Associate's use or disclosure of PHI, within a reasonable period of time after Covered Entity becomes aware of such change.

3.3 **Restrictions on Use and Disclosure.** Covered Entity agrees to notify Business Associate of any restrictions to the use or disclosure of PHI agreed to by Covered Entity in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

3.4 **Permissible Requests.** Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity.

3.5 **Safeguards.** Covered Entity shall use appropriate safeguards in accordance with 45 CFR Section 164.306 to ensure the security of PHI provided to Business Associate pursuant to the Arrangement and this Agreement, until such PHI is received by Business Associate.

3.6 **Notice of Security Incidents.** Covered Entity agrees to report promptly in writing to the Business Associate any Security Incident of which it becomes aware.

4.0 Termination of Agreement

4.1 **Term.** This Agreement shall be effective from the Effective Date until all PHI provided by or received or created for Covered Entity is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy PHI, protections are extended to such PHI in accordance with the terms of this Agreement. The term of this Agreement shall also end upon termination of the underlying Arrangement, subject, however, to the requirements of this section 4.0 for return or destruction of all PHI.

4.2 **Termination Upon Breach of Provisions Applicable to Protected Health Information.** Any other provision of this Agreement notwithstanding, this Agreement may be terminated by Covered Entity upon ten (10) days prior written notice to Business Associate in the event that Business Associate materially breaches any obligation of this Agreement and fails to cure the breach within such ten (10) day period; provided, however, that in the event that termination of this Agreement is not feasible, in Covered Entity's sole discretion, then Covered Entity shall have the right to report Business Associate's breach to the Secretary of the Department of Health and Human Services.

4.3 **Return or Destruction of Protected Health Information Upon Termination.** Upon termination of this Agreement, Business Associate shall either return to Covered Entity or destroy all PHI in Business Associate's possession or in the possession of its agents or subcontractors. Business Associate shall not retain any copies of PHI. Notwithstanding the foregoing, if Business Associate determines that returning or destroying PHI is infeasible,

Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make return or destruction infeasible, for so long as Business Associate maintains such PHI. If Business Associate elects to destroy all PHI, it shall certify in writing to Covered Entity that such PHI has been destroyed.

4.4 **Remedies.** Notwithstanding any rights or remedies set forth in this Agreement or provided by law, Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by Business Associate, any of its agents or subcontractors, or any third party who has received PHI from Business Associate.

4.5 **Judicial or Administrative Proceedings.** Either Party may terminate this Agreement, effective immediately, if (i) the other Party is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations or other security or privacy laws, or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the Party has been joined.

5.0 Miscellaneous

5.1 **Relationship of the Parties.** None of the provisions of this Agreement are intended to create or shall be deemed to create any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement between the Parties.

5.2 **Ownership of Protected Health Information.** The PHI and any related information created for or received from Covered Entity is, and will remain, the property of Covered Entity, including any and all forms thereof developed by Business Associate in the course of fulfilling its obligations pursuant to the Arrangement. Business Associate agrees that it acquires no ownership rights to or title in PHI or any related information.

5.3 **No Third Party Beneficiaries.** Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person or entity, other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

5.4 **Amendment to Comply With Law.** Business Associate and Covered Entity agree to amend this Agreement to the extent necessary to allow either Party to

comply with the Privacy Standards (45 CFR Parts 160 and 164), the Standards for Electronic Transactions (45 CFR Parts 160 and 162), and the Security Standards (45 CFR Part 142) (collectively, the "Standards") promulgated or to be promulgated pursuant to HIPAA and other applicable federal or state regulations or statutes. Business Associate and Covered Entity will fully comply with all applicable Standards and other applicable federal or state regulations or statutes and will amend this Agreement to incorporate any provisions required by the Standards, such regulations or statutes.

5.5 **Other Amendments.** This Agreement may be amended or modified only in writing signed by the Parties.

5.6 **Waiver.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation on any other occasion.

5.7 **Survival.** The respective rights and obligations of Business Associate under Sections 2.10, 2.11 and 4.0 of this Agreement shall survive the termination of this Agreement.

5.8 **Notice.** Any notice to the other party pursuant to this Agreement shall be deemed provided if sent by first class United States mail, postage prepaid, as follows:

To Covered Entity:

To Business Associate:

The above addresses may be changed by giving notice of such change in the manner provided above for giving notice.

5.9 **Effect on Arrangement.** The provisions of this Agreement shall prevail over any provisions of the Arrangement that conflict with or are inconsistent with any provision of this Agreement. All other terms of the Arrangement shall remain in full force and effect.

5.10 **Interpretation.** This Agreement shall be interpreted as broadly as necessary to implement and comply with the Privacy and Security Rule. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies with and is consistent with the Privacy Rule.

5.11 **Costs.** Each Party, at its own expense, shall provide and maintain the personnel, equipment, hardware, software, services (including without limitation telecommunications services) and testing necessary to comply with the privacy and security provisions of this Agreement.

IN WITNESS WHEREOF, the Parties' authorized representatives hereto have duly executed the Agreement.

DIRIGO HEALTH AGENCY

By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____