EXHIBIT D

Data Sharing Agreement ("Agreement")

1 **Information Covered by this Agreement.** In carrying out its duties, Contractor will be handling one or more types of private information, collectively referred to as "protected information," concerning individual State clients. "Protected information," for purposes of this Agreement, may include any or all of the following:

(a) Private data (as defined in Minnesota Statutes § 13.02, subd. 12), confidential data (as defined in Minn. Stat. § 13.02, subd. 3), welfare data (as governed by Minn. Stat. § 13.46), medical data (as governed by Minn. Stat. § 13.384), and other non-public data governed by other sections in the Minnesota Government Data Practices Act (MGDPA), Minn. Stats. Chapter 13;
(b) Health records (as governed by the Minnesota Health Records Act [Minn. Stat. §§ 144.291-144.298]);
(c) Chemical health records (as governed by 42 U.S.C. § 290dd-2 and 42 C.F.R. § 2.1 to § 2.67);
(d) Protected health information ("PHI") (as defined in and governed by the Health Insurance Portability Accountability Act ("HIPAA"), 45 C.F.R. § 160.103);
(e) Electronic Health Records (as governed by Health Information Technology for Economic and Clinical Health Act (HITECH), 42 USC 201 note, 42 USC 17931);
(f) Federal Tax Information ("FTI") (as defined by IRC § 6103);
(g) Record (as defined by the Privacy Act of 1974, 5 U.S.C. § 552a; and
(h) Other data subject to applicable State and federal statutes, rules, and regulations affecting the collection, storage, use, or dissemination of private or confidential information.

2 **Duties Relating to Protection of Information.**

(a) *Duty to ensure proper handling of information.* Contractor shall be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of protected information collected, created, used, maintained, or disclosed on behalf of State. This responsibility includes ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed above in paragraph 1.
(b) *Minimum necessary access to information.* Contractor shall comply with the "minimum necessary" access and disclosure rule set forth in the HIPAA and the MGDPA. The collection, creation, use, maintenance, and disclosure of protected information shall be limited to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." See, respectively, 45 C.F.R. §§ 164.502(b) and 164.514(d), and Minn. Stat. § 13.05 subd. 3. Furthermore, to the extent that any Protected Information is FTI, ensure that this data only be used as authorized under the Patient Protection and Affordable Care Act and restrict from use for any other purpose.
(c) *Information Requests.* Unless provided for otherwise in this Agreement, if Contractor receives a request to release the information referred to in this Clause, Contractor must immediately notify State. State will give Contractor instructions concerning the release of the data to the requesting party before the data is released.

3 **Contractor Use of Information.** Contractor shall:

(a) Not use or further disclose protected information created, collected, received, stored, used, maintained, or disseminated in the course or performance of this Agreement other than as permitted or required by this Agreement or as required by law, either during the period of this Agreement or hereafter.
(b) Use appropriate safeguards to prevent use or disclosure of the protected information by its employees, subcontractors and agents other than as provided for by this Agreement. This includes, but is not limited to, having implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentially, integrity, and availability of any electronic protected health information at rest and in transit that it creates, receives, maintains, or transmits on behalf of State.
(c) Report to State any privacy or security incident regarding the information of which it becomes aware. For purposes of this Agreement, "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Privacy incident" means violation of the Minnesota Government Data Practices Act (MGDPA) and/or the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E), including, but not limited to, improper and/or unauthorized use or disclosure of protected information, and incidents in which the confidentiality of the information maintained by it has been

breached. This report must be in writing and sent to State not more than 7 days after learning of such non-permitted use or disclosure. Such a report will at least: (1) Identify the nature of the non-permitted use or disclosure; (2) Identify the PHI used or disclosed; (3) Identify who made the non-permitted use or disclosure and who received the non-permitted or violating disclosure; (4) Identify what corrective action was taken or will be taken to prevent further non-permitted uses or disclosures; (5) Identify what was done or will be done to mitigate any deleterious effect of the non-permitted use or disclosure; and (6) Provide such other information, including any written documentation, as State may reasonably request.

(d) Consistent with this Agreement, ensure that any agents (including Contractors and subcontractors), analysts, and others to whom it provides protected information, agree in writing to be bound by the same restrictions and conditions that apply to it with respect to such information.

(e) Document such disclosures of PHI and information related to such disclosures as would be required for State to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

(f) Mitigate, to the extent practicable, any harmful effects known to it of a use, disclosure, or breach of security with respect to protected information by it in violation of this Agreement.

4 **Additional Business Associate Duties.** To the extent Contractor handles protected health information ("PHI") in order to provide health care-related administrative services on behalf of State and is a "Business Associate" of State as defined by HIPAA, Contractor further agrees to:

(a) Make available PHI in accordance with 45 C.F.R. § 164.524.

(b) Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526.

(c) Comply with the limited disclosure rules set forth in the HITECH Act, HIPAA, and the MGDPA. To the extent possible, disclosures should be in a limited data set, which is largely information with the patients' identifying information removed, "to the extent practicable." Pertinent identifiers include, name and social security number; street address, e-mail address, telephone and fax numbers; certificate/license numbers; vehicle identifiers and serial numbers; URLs and IP addresses; full face photos and any other comparable images; or medical record numbers, health plan beneficiary numbers, and other account numbers. If a limited data set is not feasible, or does not meet the use or disclosure, minimum necessary should be applied. The collection, creation, use, maintenance, and disclosure of protected information shall be limited to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." See, respectively, 45 C.F.R. §§ 164.514, 45 C.F.R. §§ 164.502(b) and 164.514(d), and Minn. Stat. § 13.05 subd. 3.

(d) Make its internal practices, books, records, policies, procedures, and documentation relating to the use, disclosure, and/or security of PHI available to State and/or the Secretary of the United States Department of Health and Human Services (HHS) for purposes of determining compliance with the Privacy Rule and Security Standards, subject to attorney-client and other applicable legal privileges.

(e) Comply with any and all other applicable provisions of the HIPAA Privacy Rule, Administrative, and Security Standards, including future amendments thereto. Develop written policies and procedures for safeguarding and securing PHI and complying with HIPAA and the HITECH Act, and other privacy laws. Designate a privacy official to be responsible for the development and implementation of its policies and procedures as required by 45 C.F.R. Part 164, Subpart E.

5 **State Use of Information.** State shall:

(a) Only release information which it is authorized by law or regulation to share with Contractor.

(b) Obtain any required consents, authorizations, or other permissions that may be necessary for it to share information with Contractor.

(c) Notify Contractor of limitations, restrictions, changes, or revocation of permission by an individual to use or disclose protected information, to the extent that such limitations, restrictions, changes or revocation may affect Contractor's use or disclosure of protected information.

(d) Not request Contractor to use or disclose protected information in any manner that would not be permitted under law if done by State.

6 **Disposition of Data upon Completion, Expiration, or Agreement Termination.** Upon completion, expiration, or termination of this Agreement, Contractor will return to State or destroy all protected information received or created on

behalf of State for purposes associated with this Agreement. A written certification of destruction or return to the State Authorized Representative is required. Contractor will retain no copies of such protected information, provided that if both parties agree that such return or destruction is not feasible, or if Contractor is required by the applicable regulation, rule or statutory retention schedule to retain beyond the life of this Agreement, Contractor will extend the protections of this Agreement to the protected information and refrain from further use or disclosure of such information, except for those purposes that make return or destruction infeasible, for as long as Contractor maintains the information.

7 **Sanctions.** In addition to acknowledging and accepting the terms set forth in the Contract Clause 9, "Indemnification." relating to liability, the parties acknowledge that violation of the laws and protections described above could result in limitations being placed on future access to protected information, in investigation and imposition of sanctions by the U.S. Department of Health and Human Services, Office for Civil Rights, and/or in civil and criminal penalties.