DEPARTMENT OF HUMAN SERVICES

DATA SHARING AND BUSINESS ASSOCIATE AGREEMENT TERMS AND CONDITIONS

This Data Sharing and Business Associate Agreement, and amendments and supplements thereto ("Agreement"), is between the State of Minnesota, acting through its Department of Human Services, Click here to enter Division, ("STATE") and Click here to enter name of party ("DATA SHARING PARTNER").

RECITALS

This Agreement sets forth the terms and conditions in which STATE will share data with and permit DATA SHARING PARTNER to Use or Disclose Protected Information that the parties are legally required to safeguard pursuant to the Minnesota Government Data Practices Act ("MGDPA") under Minnesota Statutes, chapter 13, the Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 ("HIPAA"), and other Applicable Safeguards.

The parties agree to comply with all applicable provisions of the MGDPA, HIPAA, and any other Applicable Safeguard that applies to the Protected Information.

General Description of Protected Information That Will Be Shared: EXAMPLE: "Minnesota Health Programs claims data for fiscal years 2013 through 2014". Identify data to be shared.

Purpose for Sharing Protected Information and Expected Outcomes: EXAMPLE: "Review Minnesota Health Programs to program integrity, quality, and effectiveness." Briefly describe reason for sharing.

STATE is permitted to share the Protected Information with DATA SHARING PARTNER pursuant to: Cite legal authority that permits sharing.

It is expressly agreed that DATA SHARING PARTNER is a "business associate" of STATE, as defined by HIPAA under 45 C.F.R. § 160.103, "Definitions." The Disclosure of Protected Health Information to DATA SHARING PARTNER that is subject to the Health Insurance Portability Accountability Act (HIPAA) is permitted by 45 C.F.R. § 164.502(e)(1)(i), "Standard: Disclosures to Business Associates."

It is understood by DATA SHARING PARTNER that, as a business associate under HIPAA, DATA SHARING PARTNER is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making Uses and Disclosures of Protected Health Information that are not authorized by contract or permitted by law. DATA SHARING PARTNER is also directly liable and subject to civil penalties for failing to safeguard electronic Protected Health Information in accordance with the HIPAA Security Rule, Subpart C of 45 C.F.R. Part 164, "Security and Privacy."

DEFINITIONS

A. "Agent" means DATA SHARING PARTNER'S employees, contractors, subcontractors, and other non-employees and representatives.

B. “Applicable Safeguards” means the state and federal safeguards listed in subsection 2.1.A of this Agreement.

C. “Breach” means the acquisition, access, Use, or Disclosure of unsecured Protected Health Information in a manner not permitted by HIPAA, which compromises the security or privacy of Protected Health Information.

D. “Business Associate” shall generally have the same meaning as the term “business associate” found in 45 C.F.R. § 160.103, and in reference to the party in the Agreement, shall mean DATA SHARING PARTNER.

E. “Disclose” or “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information by the entity in possession of the Protected Information.

F. “HIPAA” means the rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164.

G. “Individual” means the person who is the subject of protected information.

H. “Privacy Incident” means a violation of an information privacy provision of any applicable state and federal law, statute, regulation, rule, or standard, including those listed in the Agreement.

I. “Protected Information” means any information, regardless of form or format, which is or will be Used by STATE or DATA SHARING PARTNER under the Agreement that is protected by federal or state privacy laws, statutes, regulations, policies, or standards, including those listed in this Agreement. This includes, but is not limited to, individually identifiable information about a State, county or tribal human services agency client or a client’s family member. Protected Information also includes, but is not limited to, Protected Health Information, as defined below, and Protected Information maintained within or accessed via a State information management system, including a State “legacy system” and other State application.

J. “Protected Health Information” is a subset of Protected Information (defined above) and has the same meaning as the term “protected health information” found in 45 C.F.R. § 160.103. For the purposes of this Agreement, it refers only to that information that is received, created, maintained, or transmitted by DATA SHARING PARTNER as a Business Associate on behalf of STATE.

K. “Security Incident” means the attempted or successful unauthorized accessing, Use, or interference with system operations in an information management system or application. “Security Incident” does not include pings and other broadcast attacks on a system’s firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, provided that such activities do not result in the unauthorized exposure, viewing, obtaining, accessing, or Use of Protected Information.

L. “Use” or “Used” means any activity involving Protected Information including its creation, collection, access, acquisition, modification, employment, application, utilization, examination,

analysis, manipulation, maintenance, dissemination, sharing, Disclosure, transmission, or destruction. "Use" includes any of these activities whether conducted manually or by electronic or computerized means.

1. TERM OF AGREEMENT.

1.1 Effective date. The effective date of this Agreement is Click here to enter effective date, or the date this Agreement is signed by both parties, whichever is later.

1.2 Expiration date. The expiration date of this Agreement is Click here to enter expiration date, or until all obligations set forth in this Agreement have been satisfactorily fulfilled, whichever occurs first.

2. DUTIES.

2.1 STATE will disclose the following information to DATA SHARING PARTNER: Identify and describe data to be shared.

A. The data exchanged under the Agreement is provided to DATA SHARING PARTNER for DATA SHARING PARTNER to: Reason for sharing data.

B. STATE is permitted to share the Protected Information with DATA SHARING PARTNER pursuant to: Legal authority permitting sharing.

C. STATE will share the Protected Information by Click here to describe how STATE will share data.

2.2 DATA SHARING PARTNER shall: Click here to describe duties that are expected from the DATA SHARING PARTNER under the Agreement and specifically state how the data will be used to accomplish those tasks.

3. TIME.

The parties will perform their duties within the time limits established in this Agreement unless prior written approval is obtained from the other party.

4. CONSIDERATION AND PAYMENT.

There will be no funds obligated by either party under this Agreement. Each party will be responsible for its own costs in performing its stated duties.

5. AUTHORIZED REPRESENTATIVES AND RESPONSIBLE AUTHORITY.

5.1 State. STATE's authorized representative is Click here to enter Name, Title, and Contact Information**,** or successor. DATA SHARING PARTNER shall make any notice or contact to STATE required by this Agreement to STATE's authorized representative.

5.2 Data Sharing Partner. DATA SHARING PARTNER's Authorized Representative is Click here to enter Name, Title, and Contact Information or successor.

5.3 Information Privacy and Security. STATE's responsible party for the purposes of complying with the Applicable Safeguards in this Agreement is STATE's authorized representative. DATA SHARING PARTNER's responsible party for the purposes of complying with the Applicable Safeguards this Agreement is Click here to enter Name, Title, and Contact Information or successor.

6. INFORMATION PRIVACY AND SECURITY

DATA SHARING PARTNER and STATE must comply with the MGDPA, HIPAA, and all other Applicable Safeguards as they apply to all data provided by STATE under the Agreement, and as they apply to all data created, collected, received, stored, Used, maintained, or disseminated by DATA SHARING PARTNER under the Agreement. The civil remedies of Minn. Stat. § 13.08, "Civil Remedies," apply to DATA SHARING PARTNER and STATE. Additionally, the remedies of HIPAA apply to the release of data governed by HIPAA.

6.1 Compliance with Applicable Safeguards.

A. State and Federal Safeguards. The parties acknowledge that the Protected Information to be shared under the terms of the Agreement may be subject to one or more of the laws, statutes, regulations, rules, policies, and standards, as applicable and as amended or revised ("Applicable Safeguards"), listed below, and agree to abide by the same.

1. Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 ("HIPAA");
2. Minnesota Government Data Practices Act (Minn. Stat. Chapter 13);
3. Minnesota Health Records Act (Minn. Stat. § 144.291–144.34);
4. Confidentiality of Alcohol and Drug Abuse Patient Records (42 U.S.C. § 290dd-2, "Confidentiality of Records," and 42 C.F.R. Part 2, "Confidentiality of Substance Use Disorder Patient Records");
5. Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. § 6103, "Confidentiality and Disclosure of Returns and Return Information," and Internal Revenue Service Publication 1075;
6. U.S. Privacy Act of 1974;
7. Computer Matching Requirements (5 U.S.C. § 552a, "Records Maintained on Individuals");
8. Social Security Data Disclosure (section 1106 of the Social Security Act: 42 USC § 1306, "Disclosure of information in Possession of Social Security Administration or Department of Health and Human Services");
9. Disclosure of Information to Federal, State and Local Agencies (DIFSLA Handbook, Internal Revenue Service Publication 3373);
10. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260, "Privacy and Security of Personally Identifiable Information,");
11. NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4 (NIST.SP.800-53r4); and,
12. All state of Minnesota "Enterprise Information Security Policies and Standards."[1]

The parties further agree to comply with all other laws, statutes, regulations, rules, and standards, as amended or revised, applicable to the exchange, Use and Disclosure of data under the Agreement.

B. Statutory Amendments and Other Changes to Applicable Safeguards. The Parties agree to take such action as is necessary to amend the Agreement from time to time as is necessary to ensure, current, ongoing compliance with the requirements of the laws listed in this Section or in any other applicable law.

[1] *See* https://mn.gov/mnit/government/policies/security/

6.2 DATA SHARING PARTNER Data Responsibilities

A. Use Limitation.

1. Restrictions on Use and Disclosure of Protected Information. Except as otherwise authorized in the Agreement, DATA SHARING PARTNER may only Use or Disclose Protected Information as minimally necessary to provide the services to STATE as described in the Agreement, or as otherwise required by law, provided that such Use or Disclosure of Protected Information, if performed by STATE, would not violate the Agreement, HIPAA, or state and federal statutes or regulations that apply to the Protected Information.

2. Federal tax information. To the extent that Protected Information Used under the Agreement constitutes "federal tax information" (FTI), DATA SHARING PARTNER shall ensure that this data only be Used as authorized under the Patient Protection and Affordable Care Act, the Internal Revenue Code, 26 U.S.C. § 6103(C), and IRS Publication 1075.

B. Individual Privacy Rights. DATA SHARING PARTNER shall ensure Individuals are able to exercise their privacy rights regarding Protected Information, including but not limited to the following:

1. Complaints. DATA SHARING PARTNER shall work cooperatively and proactively with STATE to resolve complaints received from an Individual; from an authorized representative; or from a state, federal, or other health oversight agency.

2. Amendments to Protected Information Requested by Data Subject Generally. Within three (3) business days, DATA SHARING PARTNER must forward to STATE any request to make any amendment(s) to Protected Information in order for STATE to satisfy its obligations under Minn. Stat. § 13.04, "Rights of Subjects of Data," subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then DATA SHARING PARTNER must also make any amendment(s) to Protected Health Information as directed or agreed to by STATE pursuant to 45 C.F.R. § 164.526, "Amendment of Protected Health Information," or otherwise act as necessary to satisfy STATE or DATA SHARING PARTNER's obligations under 45 CF.R. § 164.526 (including, as applicable, Protected Health Information in a designated record set).

C. Background Review and Reasonable Assurances of Agents.

1. Criminal Background Check Required. DATA SHARING PARTNER and employees of DATA SHARING PARTNER accessing STATE's Protected Information must submit to STATE or provide evidence of a computerized criminal history system background check (hereinafter "CCH background check") performed within the last six (6) months before work can begin under the Agreement. "CCH background check" is defined as a background check including search of the computerized criminal history system of the Minnesota Department of Public Safety's Bureau of Criminal Apprehension.

2. Reasonable Assurances. DATA SHARING PARTNER represents that, before any Agent is allowed to Use or Disclose Protected Information, DATA SHARING

PARTNER has conducted and documented a background review of the Agent sufficient to provide DATA SHARING PARTNER with reasonable assurances that the Agent will fully comply with the terms of the Agreement and Applicable Safeguards.

3. **Documentation.** DATA SHARING PARTNER shall make available documentation required by this Section upon request by STATE.

D. Ongoing Responsibilities to Safeguard Protected Information.

1. **Privacy and Security Safeguards.** DATA SHARING PARTNER shall develop, maintain, and enforce policies, procedures, and administrative, technical, and physical safeguards that comply with the Applicable Safeguards to ensure the privacy and security of the Protected Information, and to prevent the Use or Disclosure of Protected Information, except as expressly permitted by the Agreement.

2 **Electronic Protected Information.** DATA SHARING PARTNER shall implement and maintain appropriate safeguards with respect to electronic Protected Information, and comply with Subpart C of 45 C.F.R. Part 164 (HIPAA Security Rule) with respect to prevent the Use or Disclosure other than as provided for by the Agreement.

3. **Monitoring Agents.** DATA SHARING PARTNER shall ensure that any Agent to whom DATA SHARING PARTNER Discloses Protected Information on behalf of STATE, or whom DATA SHARING PARTNER employs or retains to create, receive, Use, store, Disclose, or transmit Protected Information on behalf of STATE, agrees in writing to the same restrictions and conditions that apply to DATA SHARING PARTNER under the Agreement with respect to such Protected Information, and in accordance with 45 C.F.R. §§ 164.502, "Use and Disclosure of Protected Health Information: General Rules," subpart (e)1)(ii) and 164.308, "Administrative Safeguards," subpart (b)(2).

4. **Encryption**. According to the state of Minnesota's "Enterprise Information Security Policies and Standards,"[2] DATA SHARING PARTNER must use encryption to store, transport, or transmit Protected Information and must not use unencrypted email to transmit Protected Information.

5. **Minimum Necessary Access to Protected Information.** DATA SHARING PARTNER shall ensure that its Agents acquire, access, Use, and Disclose only the minimum necessary Protected Information needed to complete an authorized and legally permitted activity.

6. **Training and Oversight.** DATA SHARING PARTNER shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of the Agreement.

E. Responding to Privacy Incidents, Security Incidents, and Breaches. DATA SHARING PARTNER will comply with this Section for all Protected Information shared under the Agreement. Additional obligations for specific kinds of Protected Information shared under the Agreement are addressed in subsection 6.2.F, "Reporting Privacy Incidents,

[2] https://mn.gov/mnit/government/policies/security/

Security Incidents, and Breaches."

1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected Privacy Incident, Security Incident, and/or Breach, DATA SHARING PARTNER will mitigate, to the extent practicable, any harmful effect of the Privacy Incident, Security Incident, and/or Breach. Mitigation may include, but is not limited to, notifying and providing credit monitoring to affected Individuals.

2. **Investigation.** Upon discovery of any actual or suspected Privacy Incident, Security Incident, and/or Breach, DATA SHARING PARTNER will investigate to (1) determine the root cause of the incident, (2) identify Individuals affected, (3) determine the specific Protected Information impacted, and (4) comply with notification and reporting provisions of the Agreement, this Agreement, and applicable law.

3. **Corrective action.** Upon identifying the root cause of any Privacy Incident, Security Incident, and/or Breach, DATA SHARING PARTNER will take corrective action to prevent, or reduce to the extent practicable, any possibility of recurrence. Corrective action may include, but is not limited to, patching information system security vulnerabilities, sanctioning Agents, and/or revising policies and procedures.

4. **Notification to Individuals and others; costs incurred.**

    a. **Protected Information.** DATA SHARING PARTNER will determine whether notice to data subjects and/or any other external parties regarding any Privacy Incident or Security Incident is required by law. If such notice is required, DATA SHARING PARTNER will fulfill the STATE's and DATA SHARING PARTNER's obligations under any applicable law requiring notification, including, but not limited to, Minn. Stat. §§ 13.05, "Duties of Responsible Authority," and 13.055, "Disclosure of Breach in Security."

    b. **Protected Health Information.** If a Privacy Incident or Security Incident results in a Breach of Protected Health Information, as these terms are defined in this Agreement and under HIPAA, then DATA SHARING PARTNER will provide notice to Individual data subjects under any applicable law requiring notification, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404, "Notification to Individuals."

    c. **Failure to notify.** If DATA SHARING PARTNER fails to timely and appropriately notify Individual data subjects or other external parties under subparagraph (a), then DATA SHARING PARTNER will reimburse STATE for any costs, fines, or penalties incurred as a result of DATA SHARING PARTNER's failure to timely provide appropriate notification.

5. **Obligation to report to STATE.** Upon discovery of a Privacy Incident, Security Incident, and/or Breach, DATA SHARING PARTNER will report to STATE in writing as further specified in subsection 6.2.F.

    a. **Communication with authorized representative.** DATA SHARING PARTNER will send any written reports to, and communicate and coordinate as necessary with, STATE's authorized representative or designee.

b. **Cooperation of response.** DATA SHARING PARTNER will cooperate with requests and instructions received from STATE regarding activities related to investigation, containment, mitigation, and eradication of conditions that led to, or resulted from, the Security Incident, Privacy Incident, and/or Breach, and all matters pertaining to reporting and notification of a Security Incident, Privacy Incident, and/or Breach.

c. **Information to respond to inquiries about an investigation.** DATA SHARING PARTNER will, as soon as possible, but not later than forty-eight (48) hours after a request from STATE, provide STATE with any reports or information requested by STATE related to an investigation of a Security Incident, Privacy Incident, and/or Breach.

6. **Documentation.** DATA SHARING PARTNER will document actions taken under paragraphs 1 through 5 of this subsection, and retain this documentation for a minimum of six (6) years from the date it discovered the Privacy Incident, Security Incident, and/or Breach or the time period required by subsection 6.2.I, whichever is longer. DATA SHARING PARTNER shall provide such documentation to STATE upon request.

F. **Reporting Privacy Incidents, Security Incidents, and Breaches.** DATA SHARING PARTNER will comply with the reporting obligations of this Section as they apply to the kind of Protected Information involved. DATA SHARING PARTNER will also comply with subsection 6.2.E, "Responding to Privacy Incidents, Security Incidents, and Breaches," above in responding to any Privacy Incident, Security Incident, and/or Breach.

1. . **Social Security Administration Data.** DATA SHARING PARTNER will report all actual or suspected unauthorized Uses or Disclosures of Social Security Administration (SSA) data. SSA data is information protected by section 1106 of the Social Security Act.

a. **Initial report.** DATA SHARING PARTNER will, in writing, immediately report all actual or suspected unauthorized Uses or Disclosures of SSA data to STATE. DATA SHARING PARTNER will include in its initial report to STATE all information under subsections 6.2.E(1)–(4), of this Agreement that is available to DATA SHARING PARTNER at the time of the initial report, and provide updated reports as additional information becomes available.

b. **Final report.** DATA SHARING PARTNER will, upon completion of its investigation of and response to any actual or suspected unauthorized Uses or Disclosures of SSA data, or upon STATE's request in accordance with subsection 6.2.E(5), promptly submit a written report to STATE documenting all actions taken under subsections 6.2.E(1)–(4), of this Agreement.

3. . **Protected Health Information.** DATA SHARING PARTNER will report Privacy Incidents, Security Incidents, and/or Breaches involving Protected Health Information as follows:

a. **Reporting Breaches to STATE.** DATA SHARING PARTNER will report, in writing, any Breach involving Protected Health Information to STATE within five (5) calendar days of discovery, as defined in 45 C.F.R. § 164.410,

"Notification by a Business Associate," subpart (a)(2), for all Breaches involving fewer than 500 Individuals, and immediately for all Breaches involving 500 or more Individuals. These reports shall include, at a minimum, the following information:

1. Identity of each Individual whose unsecured Protected Health Information has been, or is reasonably believed by DATA SHARING PARTNER, to have been accessed, acquired, Used, or Disclosed during the incident or Breach.
2. Description of the compromised Protected Health Information.
3. Date of the Breach.
4. Date of the Breach's discovery.
5. Description of the steps taken to investigate the Breach, mitigate its impact, and prevent future Breaches.
6. Sanctions imposed on DATA SHARING PARTNER's Agents involved in the Breach.
7. All other information that must be included in notification to the Individual under 45 C.F.R. § 164.404(c).
8. Statement that DATA SHARING PARTNER has notified, or will notify, impacted Individuals in accordance with 45 C.F.R. § 164.404 and, upon the completion of said notifications, provide through documentation of the recipients, date, content, and manner of the notifications.

b. Reporting Breaches to external parties. DATA SHARING PARTNER shall timely report all Breaches involving Protected Health Information to the impacted Individuals (as specified in 45 C.F.R. § 164.404), the U.S. Department of Health and Human Services (as specified in 45 C.F.R § 164.408, "Notification to the Secretary"), and, for Breaches involving 501 or more Individuals, to the media (as specified in 45 C.F.R. § 164.406, "Notification to the Media"). As soon as possible and no later than 10 (ten) business days prior to any report to the media required by 45 C.F.R. § 164.406, DATA SHARING PARTNER shall draft and provide to STATE for its review and approval all Breach-related reports or statements intended for the media.

c. Reporting Security Incidents that do not result in a Breach to STATE. DATA SHARING PARTNER will report, in writing, all Security Incidents that do not result in a Breach, but involve systems maintaining Protected Health Information created, received, maintained, or transmitted by DATA SHARING PARTNER or its Agents on behalf of STATE, to STATE on a monthly basis, in accordance with 45 C.F.R § 164.314, "Organizational Requirements."

d. Reporting other violations to STATE. DATA SHARING PARTNER will report, in writing, any other Privacy Incident and/or violation of an Individual's privacy rights as it pertains to Protected Health Information to STATE within five (5) calendar days of discovery as defined in 45 C.F.R. § 164.410(a)(2). This includes, but is not limited to, any violation of Subpart E of 45 C.F.R. Part 164.

4. **Other Protected Information.** DATA SHARING PARTNER will report all other Privacy Incidents, Security Incidents, and/or Breaches to STATE.

   a. **Initial report.** DATA SHARING PARTNER will report all other Privacy Incidents, Security Incidents, and/or Breaches to STATE, in writing, within five (5) calendar days of discovery. If DATA SHARING PARTNER is unable to complete its investigation of, and response to, a Privacy Incident, Security Incident, and/or Breach within five (5) calendar days of discovery, then DATA SHARING PARTNER will provide STATE with all information under subsections 6.2.E(1)–(4), of this Agreement that are available to DATA SHARING PARTNER at the time of the initial report, and provide updated reports as additional information becomes available.

   b. **Final report.** DATA SHARING PARTNER will, upon completion of its investigation of and response to a Privacy Incident, Security Incident, and/or Breach, or upon STATE's request in accordance with subsection 6.2.E(5) submit in writing a report to STATE documenting all actions taken under subsections 6.2.E(1)–(4), of this Agreement.

G. **Designated Record Set—Protected Health Information.** If, on behalf of STATE, DATA SHARING PARTNER maintains a complete or partial designated record set, as defined in 45 C.F.R. § 164.501, "Definitions," upon request by STATE, DATA SHARING PARTNER shall, in a time and manner that complies with HIPAA or as otherwise directed by STATE:

1. Provide the means for an Individual to access, inspect, or receive copies of the Individual's Protected Health Information.

2. Provide the means for an Individual to make an amendment to the Individual's Protected Health Information.

H. **Access to Books and Records, Security Audits, and Remediation.** DATA SHARING PARTNER shall conduct and submit to audits and necessary remediation as required by this Section to ensure compliance with all Applicable Safeguards and the terms of the Agreement.

1. DATA SHARING PARTNER represents that it has audited and will continue to regularly audit the security of the systems and processes used to provide services under the Agreement, including, as applicable, all data centers and cloud computing or hosting services under contract with DATA SHARING PARTNER. DATA SHARING PARTNER will conduct such audits in a manner sufficient to ensure compliance with the security standards referenced in this Agreement.

2. This security audit required above will be documented in a written audit report which will, to the extent permitted by applicable law, be deemed confidential security information and not public data under the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, "General Nonpublic Data," subd. 1(a) and 2(a).

3. DATA SHARING PARTNER agrees to make its internal practices, books, audits, and records related to its obligations under the Agreement available to STATE or a STATE designee upon STATE's request for purposes of conducting a financial or security audit, investigation, or assessment, or to determine DATA SHARING PARTNER's or STATE's compliance with Applicable Safeguards, the terms of this Agreement and accounting standards. For purposes of this provision, other

authorized government officials includes, but is not limited to, the Secretary of the United States Department of Health and Human Services.

4. DATA SHARING PARTNER will make and document best efforts to remediate any control deficiencies identified during the course of its own audit(s), or upon request by STATE or other authorized government official(s), in a commercially reasonable timeframe.

I. Documentation Required. Any documentation required by this Agreement, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by DATA SHARING PARTNER, or of other matters pertinent to the execution of the Agreement, must be securely maintained and retained by DATA SHARING PARTNER for a period of six years from the date of expiration or termination of the Agreement, or longer if required by applicable law, after which the documentation must be disposed of consistent with subsection 6.6 of this Agreement.

DATA SHARING PARTNER shall document Disclosures of Protected Health Information made by DATA SHARING PARTNER that are subject to the accounting of disclosure requirement described in 45 C.R.F. 164.528, "Accounting of Disclosures of Protected Health Information," and shall provide to STATE such documentation in a time and manner designated by STATE at the time of the request.

J. Requests for Disclosure of Protected Information. If DATA SHARING PARTNER or one of its Agents receives a request to Disclose Protected Information, DATA SHARING PARTNER shall inform STATE of the request and coordinate the appropriate response with STATE. If DATA SHARING PARTNER Discloses Protected Information after coordination of a response with STATE, it shall document the authority used to authorize the Disclosure, the information Disclosed, the name of the receiving party, and the date of Disclosure. All such documentation shall be maintained for the term of the Agreement or six years after the date of the Disclosure, whichever is later, and shall be produced upon demand by STATE.

K. Conflicting Provisions. DATA SHARING PARTNER shall comply with all applicable provisions of HIPAA and with the Agreement. To extent that the parties determine, following consultation, that the terms of this Agreement are less stringent than the Applicable Safeguards, DATA SHARING PARTNER must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, DATA SHARING PARTNER must comply with the most stringent Applicable Safeguard.

L. Data Availability. DATA SHARING PARTNER, or any entity with legal control of any Protected Information provided by STATE, shall make any and all Protected Information under the Agreement available to STATE upon request within a reasonable time as is necessary for STATE to comply with applicable law.

6.3 Data Security.

A. STATE Information Management System Access. If STATE grants DATA SHARING PARTNER access to Protected Information maintained in a STATE information management system (including a STATE "legacy" system) or in any other STATE application, computer, or storage device of any kind, then DATA SHARING PARTNER agrees to comply with any additional system- or application-specific requirements as

directed by STATE.

B. **Electronic Transmission.** The parties agree to encrypt electronically transmitted Protected Information in a manner that complies with NIST Special Publications 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations"; 800-77, "Guide to IPsec VPNs"; 800-113, "Guide to SSL VPNs," or other methods validated under Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Modules." As part of its compliance with the NIST publications, and the State of Minnesota's "Enterprise Information Security Policies and Standards," DATA SHARING PARTNER must use encryption to store, transport, or transmit any Protected Information. DATA SHARING PARTNER must not use unencrypted email to send any Protected Information to anyone, including STATE.

C. **Portable Media and Devices.** The parties agree to encrypt Protected Information written to or stored on portable electronic media or computing devices in a manner that complies with NIST SP 800-111, "Guide to Storage Encryption Technologies for End User Devices."

6.4 DATA SHARING PARTNER Permitted Uses and Responsibilities.

A. **Management and Administration.** Except as otherwise limited in the Agreement, DATA SHARING PARTNER may:

1. Use Protected Health Information for the proper management and administration of DATA SHARING PARTNER or to carry out the legal responsibilities of DATA SHARING PARTNER.

2. Disclose Protected Health Information for the proper management and administration of DATA SHARING PARTNER, provided that:

    a. The Disclosure is required by law; or

    b. The Disclosure is required to perform the services provided to or on behalf of STATE or the Disclosure is otherwise authorized by STATE, and DATA SHARING PARTNER:

        i. Obtains reasonable assurances from the entity to whom the Protected Health Information will be Disclosed that the Protected Health Information will remain confidential and Used or further Disclosed only as required by law or for the purposes for which it was Disclosed to the entity; and

        ii. Requires the entity to whom Protected Health Information is Disclosed to notify DATA SHARING PARTNER of any instances of which it is aware in which the confidentiality of Protected Health Information has been Breached or otherwise compromised.

B. **Notice of Privacy Practices.** If DATA SHARING PARTNER's duties and responsibilities require it, on behalf of STATE, to obtain individually identifiable health information from Individual(s), then DATA SHARING PARTNER shall, before obtaining the information, confer with STATE to ensure that any required Notice of Privacy Practices includes the appropriate terms and provisions.

C. **De-identify Protected Health Information.** DATA SHARING PARTNER may use Protected

Health Information to create de-identified Protected Health Information provided that DATA SHARING PARTNER complies with the de-identification methods specified in 45 C.F.R. § 164.514, "Other Requirements Relating to Uses and Disclosures of Protected Health Information." De-identified Protected Health Information remains the sole property of STATE and can only be Used or Disclosed by DATA SHARING PARTNER on behalf of STATE and pursuant to the Agreement or by prior written approval of STATE.

D. Aggregate Protected Health Information. DATA SHARING PARTNER may use Protected Health Information to perform data aggregation services for STATE, and any such aggregated data remains the sole property of STATE. The DATA SHARING PARTNER must have the written approval of STATE prior to using Protected Health Information to perform data analysis or aggregation for parties other than STATE.

6.5 STATE Data Responsibilities

A. STATE shall Disclose Protected Information to DATA SHARING PARTNER only as authorized by law to DATA SHARING PARTNER.

B. STATE shall obtain any consents or authorizations that may be necessary for it to Disclose Protected Information with DATA SHARING PARTNER.

C. STATE shall notify DATA SHARING PARTNER of any limitations that apply to STATE's Use and Disclosure of Protected Information—including any restrictions on certain Disclosures of Protected Health Information requested under 45 C.F.R. § 164.522, "Rights to Request Privacy Protection for Protected Health Information," subpart (a), to which STATE has agreed and that would also limit the Use or Disclosure of Protected Information by DATA SHARING PARTNER.

D. STATE shall refrain from requesting DATA SHARING PARTNER to Use or Disclose Protected Information in a manner that would violate applicable law or would be impermissible if the Use or Disclosure were performed by STATE.

6.6 Obligations of DATA SHARING PARTNER Upon Expiration or Cancellation of the Agreement. Upon expiration or termination of the Agreement for any reason:

A. In compliance with the procedures found in the Applicable Safeguards listed in subsection 6.1.A, or as otherwise required by applicable industry standards, or directed by STATE, DATA SHARING PARTNER shall immediately destroy or sanitize (permanently de-identify without the possibility of re-identification), or return in a secure manner to STATE all Protected Information that it still maintains.

B. DATA SHARING PARTNER shall ensure and document that the same action is taken for all Protected Information shared by STATE that may be in the possession of its Agents. DATA SHARING PARTNER and its Agents shall not retain copies of any Protected Information.

C. In the event that DATA SHARING PARTNER determines that returning or destroying the Protected Information is not feasible or would interfere with its ability to carry out its legal responsibilities, maintain appropriate safeguards, and/or comply with Subpart C of 45 C.F.R. Part 164, it shall notify STATE of the specific laws, rules, policies, or other circumstances that make return or destruction not feasible or otherwise inadvisable. Upon mutual agreement of the Parties that return or destruction of Protected Information is not feasible or otherwise inadvisable, DATA SHARING PARTNER will

continue to extend the protections of the Agreement to the Protected Information and take all measures possible to limit further Uses and Disclosures of the Protected Information for so long as it is maintained by DATA SHARING PARTNER or its Agents.

D. DATA SHARING PARTNER shall document and verify in a written report to STATE the disposition of Protected Information. The report shall include at a minimum the following information:

1. A description of all Protected Information that has been sanitized or destroyed, whether performed internally or by a service provider;

2. The method by which, and the date when, the Protected Data were destroyed, sanitized, or securely returned to STATE; and

3. The identity of organization name (if different than DATA SHARING PARTNER), and name, address, and phone number, and signature of Individual, that performed the activities required by this Section.

E. Documentation required by this Section shall be made available upon demand by STATE.

F. Any costs incurred by DATA SHARING PARTNER in fulfilling its obligations under this Section will be the sole responsibility of DATA SHARING PARTNER.

7. INSURANCE REQUIREMENTS

7.1 Network Security and Privacy Liability Insurance. DATA SHARING PARTNER shall, at all times during the term of the Agreement, keep in force a network security and privacy liability insurance policy. The coverage may be endorsed on another form of liability coverage or written on a standalone policy.

DATA SHARING PARTNER shall maintain insurance to cover claims which may arise from failure of DATA SHARING PARTNER's security or privacy practices resulting in, but not limited to, computer attacks, unauthorized access, Disclosure of not public data including but not limited to confidential or private information or Protected Health Information, transmission of a computer virus, or denial of service. DATA SHARING PARTNER is required to carry the following **minimum** limits:

$2,000,000 per occurrence

$2,000,000 annual aggregate

8. INTERPRETATION

8.1 Any ambiguity in this Agreement shall be interpreted to permit compliance with all Applicable Safeguards.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.

By signing below, the parties agree to the terms and conditions contained in this AGREEMENT.

APPROVED:

1. **DATA SHARING PARTNER**

DATA SHARING PARTNER certifies that the appropriate person(s) have executed the Agreement on behalf of DATA SHARING PARTNER as required by applicable articles, by-laws resolutions or ordinances.

By:
Printed Name:
Title:
Date:

2. **STATE AGENCY**
By (with delegated authority):
Printed Name:
Title:
Date:

Distribution: (copy of fully executed contract to each)
Contracting and Legal Compliance Division
Data Sharing Partner
State Authorized Representative