MNsure Certified Application Counselor Services Agreement Attachment B

State of Minnesota

This Attachment sets forth the terms and conditions in which State will share data with and permit Certified Application Counselor (CAC) to Use or disclose Protected Information that the parties are legally required to safeguard pursuant to the Minnesota Data Practices Act 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 laws.

DEFINITIONS

A. "Agent" means CAC's employees, contractors, subcontractors, and other non-employees and representatives.

B. "Applicable Safeguards" means the state and federal provisions listed in Section 2.1 of this Attachment.

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" at 45 C.F.R. § 160.103, and in reference to the party in the Agreement and this Attachment, shall mean CAC.

E. "Agreement" means the Grant Services Agreement between State and CAC.

F. "Disclose," "Disclosed," and "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.

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

H. "Individual" means the person who is the subject of protected information.

I. "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 and this Attachment.

J. "Protected information" means any information that is or will be Used by State or CAC under the Agreement that is protected by federal or state privacy laws, statutes, regulations or standards, including those listed in this Attachment. 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.

K. "Protected health information" is a subset of "individually identifiable health information" in accordance with 45 C.F.R. § 160.103, but for purposes of this Attachment refers only to that information that is received, created, maintained, or transmitted by CAC as a business associate on behalf of DHS. Protected health information is a specific subset of protected information as defined above.

L. "Security incident" means the attempted or successful unauthorized Use or the 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 Use of Protected Information.

M. "Use" or "Used" means any activity by the parties during the duration of the Agreement involving protected information including its creation, collection, access, use, 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.

N. "User" means an agent of either party, who has been authorized to use protected information.

1. INFORMATION EXCHANGED

1.1 This Attachment governs the data that will be exchanged pursuant to the CAC performing the services described in the Agreement. The data exchanged under the Agreement may include the following data elements about an Individual: name, address, phone number, email address, date of birth, social security number, age, sex, gender, income, medical information (e.g., health diagnoses, health conditions, and healthcare treatments), and human services program eligibility status. This data may be classified as:

(a) Private data (as defined in Minn. Stat. § 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 "not public" data (as defined in Minn. Stat. § 13.02, subd. 8a) governed by other sections in the Minnesota Government Data Practices Act (MGDPA), Minn. Stats. Chapter 13;
(b) Protected health information ("PHI") (as defined in and governed by the Health Insurance Portability and Accountability Act ("HIPAA") and 45 C.F.R. § 160.103);
(c) Records (as defined by the Privacy Act of 1974 at 5 U.S.C. § 552a(a)(4));
(d) Other data subject to applicable state and federal statutes, rules, and regulations affecting the collection, storage, Use, or dissemination of private or confidential information.

1.2 State is permitted to share the Protected Information with the CAC pursuant to Minnesota Statutes, section 62V.06, subdivision 5; 45 CFR §§ 164.506(c), and 164.512, in order for the CAC to help State perform the duties described in the grant services agreement, which is primarily to help State guide Minnesota residents through the process of enrolling in health insurance options available through State (MNsure).

2. INFORMATION PRIVACY AND SECURITY

The CAC and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. § 13, and the Health Insurance Portability Accountability Act ["HIPAA"], 45 C.F.R. § 164.103, et seq., as it applies to all data provided by State under the Agreement, and as it applies to all data created, collected, received, stored, Used, maintained, or disseminated by the CAC under the Agreement. The civil remedies of Minn.

Stat. § 13.08 apply to the CAC and State. Additionally, the remedies of HIPAA apply to the release of data governed by that Act.

2.1 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 of the following laws, statutes, regulations, rules, and standards, as applicable ("Applicable Safeguards"). The parties agree to comply with all rules, regulations and laws, including as amended or revised, applicable to the exchange, Use and Disclosure of data under the Agreement, including:

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. U.S. Privacy Act of 1974;
4. Computer Matching Requirements (5 U.S.C. 552a)
5. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260), and
6. All State of Minnesota "Enterprise Information Security Policies and Standards"[1]

(b) **Statutory Amendments and Other Changes to Applicable Safeguards.** The Parties agree to take such action as is necessary to amend the Agreement and this Attachment 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.

2.2 CAC Data Responsibilities

(a) **Use Limitation.**

1. **Restrictions on Use and Disclosure of Protected Information.** Except as otherwise authorized in the Agreement or this Attachment, the CAC may only Use or Disclose Protected Information as necessary to provide the services to State as described herein, or as otherwise required by law, provided that such Use or Disclosure of Protected Information, if performed by State, would not violate the Agreement, this Attachment, HIPAA, or other 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), the CAC 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 I075.

(b) **Individual Privacy Rights.** The CAC shall ensure Individuals are able to exercise their privacy rights regarding Protected Information, including but not limited to the following:

1. **Complaints.** The CAC shall work cooperatively 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 ten (10) business days, the CAC 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, subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then the CAC 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 or otherwise act as necessary to satisfy State or the CAC'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 Required of Agents.**

1. Criminal Background Check Required. All employees, agents and volunteers of the CAC who are seeking certification to be a MNsure-certified certified application counselor and

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

will be accessing State's Protected Information must undergo a computerized criminal history system background check.

2. **Reasonable Assurances.** The CAC represents that, before its Agents are allowed to Use or Disclose Protected Information, the CAC has conducted and documented a background review of such Agents sufficient to provide the CAC with reasonable assurances that the Agent will comply with the terms of the Agreement, this Attachment and Applicable Safeguards.
3. **Documentation.** The CAC shall make available documentation required by this Section upon request by State.

(d) **Ongoing Responsibilities to Safeguard Protected Information.**

1. **Privacy and Security Policies.** The CAC shall develop, maintain, and enforce policies, procedures, and administrative, technical, and physical safeguards to ensure the privacy and security of the Protected Information.
2. **Electronic Protected Information.** The CAC shall implement and maintain appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 (HIPAA Security Rule) with respect to electronic Protected Information, including electronic Protected Health Information, to prevent the Use or Disclosure other than as provided for by the Agreement or this Attachment.
3. **Encryption**. According to the State of Minnesota's "Enterprise Information Security Policies and Standards," the CAC must use encryption to store, transport, or transmit any Protected Information. The CAC must not use unencrypted email to send any of the State data described in this subsection to anyone.
4. **Monitoring Agents.** The CAC shall ensure that any contractor, subcontractor, or other agent to whom the CAC discloses Protected Information on behalf of State, or whom the CAC employs or retains to create, receive, Use, store, Disclose, or transmit Protected Information on behalf of State, agrees to the same restrictions and conditions that apply to the CAC under the Agreement and this Attachment with respect to such Protected Information, and in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2).
4. **Minimum Necessary Access to Protected Information.** The CAC shall ensure that its Agents Use only the minimum necessary Protected Information needed to complete an authorized and legally permitted activity.
5. **Training.** The CAC shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of the Agreement and this Attachment.

(e) **Responding to Privacy Incidents, Security Incidents, and Breaches.** The CAC 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 Section 2.2(F).

1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected privacy incident, security incident, or breach, the CAC will mitigate, to the extent practicable, any harmful effect of the privacy incident, security incident, 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, or breach, the CAC 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 Attachment and applicable law.
3. **Corrective action.** Upon identifying the root cause of any privacy incident, security incident, or breach, the CAC 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, employee sanctions, or revising policies and procedures.
4. **Notification to Individuals and others; costs incurred.**
    A. **Protected Information.** The CAC and State will coordinate to 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, the CAC will comply with State's and the CAC's obligations under any applicable law

requiring notification, including, but not limited to, Minn. Stat. §§ 13.05 and 13.055.

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 Attachment, then the CAC will provide notice to individual data subjects under any applicable law requiring notification in coordination with State, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404.

C. **Failure to notify.** If the CAC fails to notify individual data subjects or other external parties under subparagraphs (a) and (b), then the CAC will reimburse State for any costs incurred as a result of the CAC's failure to provide notification.

5. **Obligation to report to State.** Upon discovery of a privacy incident, security incident, or breach, the CAC will report to State in writing as specified in Section 2.2(F).

A. **Communication with authorized representative.** The CAC will send any written reports to, and communicate and coordinate as necessary with, State's authorized representative.

B. **Cooperation of response.** The CAC 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, or breach.

C. **Information to respond to inquiries about an investigation.** The CAC 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, or breach.

6. **Documentation.** The CAC will document actions taken under paragraphs 1 through 5 of this Section, and provide such documentation to State upon request.

(f) **Reporting Privacy Incidents, Security Incidents, and Breaches.** The CAC will comply with the reporting obligations of this Section as they apply to the kind of protected information involved. The CAC will also comply with Section 2.2(E) above in responding to any privacy incident, security incident, or breach.

1. **Protected Health Information.** The CAC will report breaches and security incidents involving protected health information to State and other external parties. The CAC will notify State, in writing, of (1) any breach or suspected breach of protected health information; (2) any security incident; or (3) any violation of an Individual's privacy rights as they involve protected health information created, received, maintained, or transmitted by the CAC or its Agents on behalf of State.

A. **Breach reporting.** The CAC will report, in writing, any breach of protected health information to State within five (5) business days of discovery, in accordance with 45 C.F.R § 164.410.

Content of report to State. Reports to the authorized representative regarding breaches of protected health information will include:

a. Identities of the Individuals whose unsecured Protected Health Information has been breached.
b. Date of the breach and date of its discovery.
c. Description of the steps taken to investigate the breach, mitigate its effects, and prevent future breaches.
d. Sanctions imposed on members of the CAC's workforce involved in the breach.
e. Other available information that is required to be included in notification to the Individual under 45 C.F.R. § 164.404(c).
f. Statement that the CAC has notified, or will notify, affected data subjects in accordance with 45 C.F.R. § 164.404.

B. **Security incidents resulting in a breach.** The CAC will report, in writing, any security incident that results in a breach, or suspected breach, of protected health information to State within five (5) business days of discovery, in accordance with 45 C.F.R § 164.314 and 45 C.F.R § 164.410.

C. **Security incidents that do not result in a breach.** The CAC will report all security incidents that do not result in a breach, but involve systems maintaining protected

health Information created, received, maintained, or transmitted by the CAC or its Agents on behalf of State, to State on a monthly basis, in accordance with 45 C.F.R § 164.314.

D. **Other violations.** The CAC will report any other violation of an Individual's privacy rights as it pertains to protected health information to State within five (5) business days of discovery. This includes, but is not limited to, violations of HIPAA data access or complaint provisions.

E. **Reporting to other external parties.** The CAC will report all breaches of protected health information to the federal Department of Health and Human Services in coordination with State, as specified under 45 C.F.R 164.408. If a breach of protected health information involves 500 or more Individuals:
   a. The CAC will immediately notify State.
   b. The CAC will coordinate with State to report to the news media and federal Department of Health and Human Services in accordance with 45 C.F.R. §§ 164.406-408.

F. **Other Protected Information.** The CAC will report all other privacy incidents and security incidents to State.
   a. **Initial report.** The CAC will report all other privacy and security incidents to State, in writing, within five (5) days of discovery. If the CAC is unable to complete its investigation of, and response to, a privacy incident or security incident within five (5) days of discovery, then the CAC will provide State with all information under Section 2.2(E)(1)-(4), of this Attachment that are available to the CAC at the time of the initial report.
   b. **Final report.** The CAC will, upon completion of its investigation of and response to a privacy incident or security incident, or upon State's request in accordance with Section 2.2(E)(5) submit in writing a report to State documenting all actions taken under Section 2.2(E)(1)-(4), of this Attachment.

(g) **Protected Health Information Designated Record Set.** If, on behalf of State, the CAC maintains a complete or partial designated record set, as defined in 45 C.F.R. § 164.501, upon request by State, the CAC shall:
   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.
   3. Provide the means for access and amendment in the time and manner that complies with HIPAA or as otherwise directed by State.

(h) **Access to Books and Records, Security Audits, and Remediation.** The CAC 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 and this Attachment.
   1. The CAC 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 and this Attachment, including, as applicable, all data centers and cloud computing or hosting services under agreement with the CAC. The CAC will conduct such audits in a manner sufficient to ensure compliance with the security standards referenced in this Attachment.
   2. This security audit required above 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, subd. 1(a) and 2(a).
   3. The CAC agrees to make its internal practices, books, and records related to its obligations under the Agreement and this Attachment 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 the CAC's or State's compliance with Applicable Safeguards, the terms of this Attachment 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. The CAC 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 Attachment, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by the CAC, or of other matters pertinent to the execution of the Agreement, must be securely maintained and retained by the CAC for a period of six (6) 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 Section 2.6 of this Attachment.

The CAC shall document disclosures of Protected Health Information made by the CAC that are subject to the accounting of disclosure requirement described in 45 C.R.F. 164.528, 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 the CAC or one of its Agents receives a request to disclose Protected Information, the CAC shall inform State of the request and coordinate the appropriate response with State. If the CAC 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 and shall be produced upon demand by State.

(l) **Conflicting Provisions.** The CAC shall comply with all applicable provisions of HIPAA and with the Agreement and this Attachment. To extent that the parties determine, following consultation, that the terms of this Attachment are less stringent than the Applicable Safeguards, the CAC must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, the CAC must comply with the most stringent Applicable Safeguard.

(m) **Data Availability.** The CAC, or any entity with legal control of any protected information provided by State, shall make any and all protected information under the Agreement and this Attachment available to State upon request within a reasonable time as is necessary for State to comply with applicable law.

2.3 **Data Security.**

(a) **State Information Management System Access.** If State grants the CAC 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 the CAC 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 others methods validated under Federal Information Processing Standards (FIPS) 140-2.

(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.

2.4 **CAC Permitted Uses and Responsibilities.**

(a) **Management and Administration.** Except as otherwise limited in the Agreement or this Attachment, the CAC may:

1. Use Protected Health Information for the proper management and administration of the CAC or to carry out the legal responsibilities of the CAC.
2. Disclose Protected Health Information for the proper management and administration of the CAC, 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 the CAC:
    a. Obtains reasonable assurances, in the form of a data sharing agreement, from the entity to whom the Protected Health Information will be disclosed that the Protected Health Information will remain confidential, and will not be Used or Disclosed other than for the agreed services or the authorized purposes; and
    b. The CAC requires the entity to whom Protected Health Information is disclosed to notify the CAC of any compromise to the confidentiality of Protected Health Information of which it becomes aware.

(b) **Notice of Privacy Practices.** If the CAC's duties and responsibilities require it, on behalf of State, to obtain individually identifiable health information from Individual(s), then the CAC 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.** The CAC may Use Protected Health Information to create de-identified Protected Health Information provided that the CAC complies with the de-identification methods specified in 45 C.F.R. § 164.514.

(d) **Aggregate Protected Health Information.** The CAC may Use Protected Health Information to perform data aggregation services for State. The Use of Protected Health Information by the CAC to perform data analysis or aggregation for parties other than State must be expressly approved by State.

2.5 **State Data Responsibilities**

(a) State shall disclose Protected Information only as authorized by law to the CAC for its Use or Disclosure.

(b) State shall obtain any consents or authorizations that may be necessary for it to disclose Protected Information with the CAC.

(c) State shall notify the CAC of any limitations that apply to State's Use and Disclosure of Protected Information that would also limit the Use or Disclosure of Protected Information by the CAC.

(d) State shall refrain from requesting the CAC 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.

2.6 **Obligations of the CAC Upon Expiration or Cancellation of the Agreement.** Upon expiration or termination of the Agreement for any reason:

(a) The CAC shall retain only that Protected Health Information which is necessary for the CAC to continue its proper management and administration or to carry out its legal responsibilities, and maintain appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information to prevent the impermissible Use or Disclosure of any retained Protected Health Information for as long as the CAC retains the Protected Health Information.

(b) For all other Protected Information, in compliance with the procedures found in the Applicable Safeguards listed in Section 2.1, or as otherwise required by applicable industry standards, or directed by State, the CAC 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.

(c) The CAC 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 contractors, subcontractors, or agents. The CAC and its contractors, subcontractors, or agents shall not retain copies of any Protected Information.

(d) In the event that the CAC cannot reasonably or does not return or destroy Protected Information, it shall notify State of the specific laws, rules or policies and specific circumstances applicable to its retention, and continue to extend the protections of the Agreement and this Attachment and take all measures possible to limit further Uses and Disclosures of the client

data for so long as the CAC or its contractors, subcontractors, or agents maintain the Protected Information.

(e) Documentation required by this Section shall be made available upon demand by State.

(f) Any costs incurred by the CAC in fulfilling its obligations under this Section will be the sole responsibility of the CAC.