DHS OF MINNESOTA DEPARTMENT OF HUMAN SERVICES INTERAGENCY AGREEMENT WORKSHEET (Not Part of the Agreement)

Originator of agreement, complete this section:

Total amount of interagency agreement: $___________

Proposed Start Date: 10_/ _1__/ _21_

Proposed End Date:_06_ /30_/ _23_

SFY__ - SWIFT FinDeptID: H55EB __ __ __ __ __ $__________amount

If multiple FinDeptID's will be used to fund this, fill that in below and then define the split between funds.

SFY__ - SWIFT FinDeptID: H55EB__ __ __ __ __$__________amount

SFY__ - SWIFT FinDeptID: H55EB__ __ __ __ __$__________amount

Reference the contract number and purchase order number assigned below when processing invoices for this agreement. Send invoices to FOD – 0940

Contract Coordinator, complete this section:

SWIFT Vendor # for Other State Agency: __H60000000___________

SWIFT Contract #: IAK % 201563____________

SWIFT Purchase Order #:___N/A__________________

Buyer Initials:________Date Encumbered:_____________

Individual signing certifies that funds have been encumbered as required by MS § 16A15.

INTERAGENCY AGREEMENT between DHS and MNsure for MNsure Participation in the Administration of the Minnesota State Plan for Services Under Title XIX

Recitals:

WHEREAS, the Department of Human Services, hereinafter DHS, is empowered to enter into interagency agreements pursuant to Minnesota Statutes § 471.59, Subdivision 10; and

WHEREAS, MNsure is empowered to enter into interagency agreements pursuant to Minnesota Statutes § 471.59, Subdivision 10; and

WHEREAS, DHS is designated as the Medicaid Agency for the State of Minnesota and, as such, is responsible for management and oversight of Medical Assistance (MA), which is Minnesota's Medicaid program; and

WHEREAS, The day-to-day operations of MNsure play an important role in the Department of Human Services' outreach and enrollment strategies for Minnesotans seeking the services of public health coverage programs and services, including MinnesotaCare and Medicaid; and

WHEREAS, DHS and MNsure are formally recognizing that work performed by MNsure benefits public health programs and MNsure expenditures will be included, as necessary, in DHS' public assistance, cost allocation plan, and operational advance planning documents.

NOW, THEREFORE, it is agreed:

1. Duties:

1.1 MNsure's Duties:

MNsure shall: help DHS to outreach, identify, intake, accept, determine eligibility for, and formally enroll eligible individuals and their families into the entire range of public and private health insurance programs in Minnesota, including individual qualified health insurance plans, the basic health insurance plan (MinnesotaCare), and medical assistance services available for those qualifying for Medicaid.

MNsure shall provide a variety of services related to Medicaid eligibility determination and enrollment activities including, but not limited to application, on-going case maintenance and renewal activities, policy, outreach and post-eligibility activities, and other activities necessary for administration of the state plan for services under Title XIX.

1.2. DHS's DUTIES:

DHS shall: obtain annual appropriations for the ongoing operation of MNsure, and shall claim the federal share of any eligible expenditures via operation of its amended public assistance cost allocation plan and operational advance planning document.

2. CONSIDERATION AND TERMS OF PAYMENT

2.1 Consideration. Consideration for all services performed by MNsure pursuant to this agreement shall be paid by DHS as follows: There is no encumbrance under this agreement. The basis for billing will be the operational advance planning document and the quarterly operation of the public assistance cost allocation plan. It is further understood that any billing will be based on the actual cost incurred.

2.2 Terms of Payment. Payment shall be made to MNsure from DHS within 30 days after DHS has completed its quarterly COCAS procedure.

3. Conditions of Payment. All services provided by MNsure pursuant to this agreement shall be performed to the satisfaction of DHS, as determined at the sole discretion of its authorized representative.

4. Terms of Agreement. This agreement shall be effective on October 1, 2021 **or upon the date that the final required signature is obtained, pursuant to Minnesota Statutes, section 16C.05, subdivision 2, whichever occurs later**, and shall remain in effect through June 30, 2023, or until all obligations set forth in this agreement have been satisfactorily fulfilled, whichever occurs first.

5. Cancellation. This agreement may be canceled by the DHS or MNsure at any time, with or without cause, upon thirty (30) days written notice to the other party. In the event of such a cancellation, the MNsure shall be entitled to payment, determined on a pro rata basis, for work or services satisfactorily performed.

6. Authorized Representatives. DHS's authorized representative for the purposes of administration of this agreement is Dave Greeman or successor. MNsure's authorized representative for the purposes of administration of this agreement is Kari Koob, CFO, or successor. Each representative shall have final authority for acceptance of services of the other party and shall have responsibility to insure that all payments due to the other party are made pursuant to the terms of this agreement.

7. Assignment. Neither MNsure nor DHS shall assign or transfer any rights or obligations under this agreement without the prior written consent of the other party.

8. Amendments. Any amendments to this agreement shall be in writing, and shall be executed by the same parties who executed the original agreement, or their successors in office.

9. Liability. MNsure and DHS agree that each party will be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other and the results thereof. MNsure and DHS liability shall be governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, section 3.736, and other applicable law.

10. INFORMATION PRIVACY AND SECURITY.

Information Privacy and Security shall be governed by the existing Data Sharing and Business Associate Agreement between MNsure and DHS, identified as DSK %187696, and any succeeding Data Sharing Agreement, which is incorporated into this agreement by reference.

11. Other Provisions.

None.

IN WITNESS WHEREOF, the parties have caused this contract to be duly executed intending to be bound thereby

APPROVED:

1. MNsure

DocuSigned by:

By: Kari Koob

F3466CF591CC40D...

Title: CFO

Date: 9/29/2021

2. DHS

DocuSigned by:

By: Charles Johnson

E336517A7B0D415...

With delegated authority

Title: Deputy Commissioner

Date: 9/29/2021

Distribution:
DHS – Original (fully executed) contract
MNsure
Contracting & Legal Compliance, Contracts Unit- #0238

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 Department of Human Services("DHS") and Minnesota Insurance Marketplace a/k/a MNsure ("MNsure"), collectively referred to as "parties".

RECITALS

This Agreement sets forth the terms and conditions in which parties will share data with and permit the other party 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.

DHS is the primary state agency to help people meet their basic needs by providing or administering a variety of services for children, people with disabilities, and older Minnesotans.

DHS is the designated Medicaid Agency for the state of Minnesota and is responsible for the management and oversight of Medical Assistance (MA), MinnesotaCare, and other Minnesota Health Care Programs.

DHS is a "health care provider" and a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA) pursuant to 45 C.F.R. § 160.103.

MNsure is the state of Minnesota's state health benefit exchanged as described in section 1311 of the Patient Protection and Affordable Care Act, Public Law 111-148.

MNsure and DHS share decision-making in conjunction with MNIT Services for the Minnesota Eligibility Technology System (METS).

To carry out their duties under the Interagency Agreements between the parties to implement and administer the Minnesota Insurance Marketplace and Minnesota Health Care Programs ("Interagency Agreements"), MNsure and DHS are required to share Protected Information and Protected Health Information with each other, as defined in this Agreement.

MNsure is permitted to share the protected information with DHS pursuant to Minnesota Statutes, section 62V.06, subdivisions 5(a)(4) and 5(b)(4) and 45 C.F.R. § 155.260.

MNsure agrees it is a “business associate” of DHS, as defined by HIPAA under 45 C.F.R. § 160.103, “Definitions,” for the limited purpose of carrying out health care eligibility operations and administration on behalf of DHS. The Protected Health Information disclosed to MNsure 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.”

MNsure and DHS are directly liable and may be 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.”

DHS is permitted to share protected health information with MNsure by 45 C.F.R. §§ 164.502(a)(1)(ii) and 164.506(c)(1) for DHS’ health care operations.

Minnesota Statutes, section 13.46, subdivision 1(c), allows DHS to enter into agreements to make the other entity part of the “Welfare System.” It is the intention that MNsure be made part of the welfare system for the limited purpose described in the Interagency Agreements and this Agreement.

Pursuant to Minnesota Statutes, section 13.46, subdivision 2(a)(5), DHS is permitted to release private data on individuals to personnel of the welfare system who require the data to verify an individual’s identity, the amount of assistance, and the need to provide services to an individual or family across programs; and evaluate the effectiveness of programs.

Pursuant to Minnesota Statutes, section 13.46, subdivision 2(a)(6), DHS is permitted to release private data on individuals to administer federal funds and programs.

Therefore, the parties agree as follows:

DEFINITIONS

A. "Agent" means the parties’ employees, contractors, subcontractors, and other non-employees and representatives.

B. “Applicable Safeguards” means the state and federal safeguards listed in subsection 6.1.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 MNsure.

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 DHS or MNsure 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 between DHS and MNsure as a Business Associate for the limited purpose of carrying out health care eligibility operations and administration on behalf of DHS.

K. “Responsible Party” is the agency whose employee, volunteer, agent, vendor, contractor or subcontractor actions causes the Breach, Privacy Incident, and/or Security Incident. For purposes of this Agreement, if the parties to this Agreement disagree or cannot determine the cause of an incident, or if a third party caused a security incident, both parties to this Agreement will be deemed the Responsible Party for the Breach, Privacy Incident, and/or Security Incident, and the parties will work cooperatively to agree on one party to take the lead with coordination and assistance from the other party.

L. “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.

M. “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.

N. “User” means an agent of either party, who has been authorized to use Protected Information.

1. TERM OF AGREEMENT.

1.1 Effective date. The effective date of this Agreement is **January 1, 2021**.

1.2 Expiration date. The expiration date of this Agreement is **December 31, 2023**, or until all obligations set forth in this Agreement have been satisfactorily fulfilled, whichever occurs first.

2. INFORMATION EXCHANGED.

2.1 This Agreement shall govern the data that will be exchanged between MNsure and DHS, which may include:

A. patient data relating to DHS' Minnesota Health Care Programs (MHCP);

B. the provision of health care to MHCP beneficiaries and MNsure clients;

C . past, present, or future payment for the provision of health care to MHCP beneficiaries and MNsure clients;

D. data on individuals participating in MNsure as defined in Minnesota Statutes, section 62V.06;

E. data on employers participating in MNsure; and

F. "not public data" as defined in Minnesota Statutes, section 13.02.

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.

5.1 DHS. DHS's authorized representative is **Donna Watz, Deputy General Counsel Chief Privacy Official,** donna.m.watz@state.mn.us, or her successor. MNsure shall make any notice or contact to DHS required by this Agreement to DHS's authorized representative.

5.2 MNsure. MNsure's Authorized Representative is **Emily Cleveland, Legal Director and Privacy Officer**, emily.j.cleveland@state.mn.us, or her successor. DHS shall make any notice or contact to MNsure required by this Agreement to MNsure's authorized representative.

6. INFORMATION PRIVACY AND SECURITY

MNsure and DHS must comply with the MGDPA, HIPAA, and all other Applicable Safeguards as they apply to all data provided by MNsure or DHS under this Agreement, and as they apply to all data created, collected, received, stored, used, maintained, or disseminated by MNsure or DHS under this Agreement. The civil remedies of Minn. Stat. § 13.08, "Civil Remedies," apply to MNsure and DHS. 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. Medicaid Information Safeguards (42 C.F.R. § 431 Subpart F);
3. Minnesota Government Data Practices Act (Minn. Stat. Chapter 13);
4. Minnesota Health Records Act (Minn. Stat. § 144.291–144.34);
5. Data Practices section of the MNsure Act (Minn. Stat § 62V.06)
6. 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");
7. 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;
8. U.S. Privacy Act of 1974;
9. Computer Matching Requirements (5 U.S.C. § 552a, "Records Maintained on Individuals");
10. 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");
11. Disclosure of Information to Federal, State and Local Agencies (DIFSLA Handbook, Internal Revenue Service Publication 3373);
12. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260, "Privacy and Security of Personally Identifiable Information,");
13. NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4 (NIST.SP.800-53r4); and,
14. 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.

6.2 The Parties' Data Responsibilities

A. **Use of Protected Information.** Each party shall:

1. disclose Protected Information only as authorized by law to the other party for its use or disclosure;

2. obtain any consent or authorization that may be necessary for it to disclose Protected Information with the other party; and
3. refrain from asking the other party to use or disclose Protected Information in a manner that would violate applicable standards or would be impermissible if the use or disclosure were performed by the party.

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

B. **Use Limitation.**

1. **Restrictions on Use and Disclosure of Protected Information.** Except as otherwise authorized in the Agreement, the parties may only use or disclose Protected Information as minimally necessary to provide the services to the other party as described in the Agreement, or as otherwise required by law, provided that such use or disclosure of Protected Information, if performed by the party, 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), both parties 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, and IRS Publication 1075.

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

1. **Complaints.** The parties shall work cooperatively and proactively with each other 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, one party must forward to the other party any request to make any amendment(s) to Protected Information in order for the parties to satisfy their obligations under Minnesota Statutes, section 13.04, "Rights of Subjects of Data," subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then the parties must also make any amendment(s) to Protected Health Information as directed or agreed to by the parties pursuant to 45 C.F.R. § 164.526, "Amendment of Protected Health Information," or otherwise act as necessary to satisfy DHS or MNsure's obligations under 45 CF.R. § 164.526 (including, as applicable, Protected Health Information in a designated record set).

D. **Background Review and Reasonable Assurances of Agents.**

1. **Reasonable Assurances.** Each party represents that, before any Agent is allowed to Use or Disclose Protected Information, each party has conducted and documented a background review of the Agent sufficient to provide the other party with reasonable assurances that the Agent will fully comply with the terms of the Agreement and Applicable Safeguards.

2. **Documentation.** Each party shall make available documentation required by this Section upon request.

E. **Ongoing Responsibilities to Safeguard Protected Information.**

1. **Privacy and Security Safeguards.** Each party 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.** Each party 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.** Each party shall ensure that any Agent to whom the party Discloses Protected Information on behalf of the other party, or whom the party employs or retains to create, receive, Use, store, Disclose, or transmit Protected Information on behalf of the other party, agrees in writing to the same restrictions and conditions that apply to the party under the Agreement with respect to such Protected Information; and, for protected health information, 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] both parties 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.** Each party 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.** Each party shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of the Agreement.

F. **Responding to Privacy Incidents, Security Incidents, and Breaches.** Each party will comply with this Section for all Protected Information shared under the Agreement. Each party will coordinate and cooperate with one another in responding to and handling any privacy incident, security incident, and/or breach. Additional obligations for specific kinds of Protected Information shared under the Agreement are addressed in subsection 6.2.G, "Reporting Privacy Incidents, Security Incidents, and Breaches."

1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected Privacy Incident, Security Incident, and/or Breach, the Responsible Party 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, the Responsible Party 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

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

applicable law.

3. **Corrective action.** Upon identifying the root cause of any Privacy Incident, Security Incident, and/or Breach, the Responsible Party 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.** The Responsible Party 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, the Responsible Party will fulfill its obligations under any applicable law requiring notification, including, but not limited to, Minnesota Statutes, sections 13.05, "Duties of Responsible Authority," and 13.055, "Disclosure of Breach in Security." If the incident is a "breach of the security of the data," as defined by Minnesota Statutes, section 13.055, the responsible party shall also be responsible for completing the requisite investigation report.

   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 the Responsible Party 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. **Notification to CMS**. MNsure will serve as the point of contact and notify Centers for Medicare & Medicaid Services (CMS) of incidents related to METS pursuant to the Computer Matching Agreement between CMS and State-Based Administering Entities for the Disclosure of Insurance Affordability Programs Information under the Patient Protection and Affordable Care Act.

   d. **Notification to OLA.** The Responsible Party shall report any Privacy Incident, Security Incident, and or Breach to the Minnesota Office of Legislative Auditor as required by Minnesota Statutes, section 3.971, subdivision 9.

   e. **Failure to notify.** If either party incurs costs or is subject to fines or penalties due to the other party's failure to timely and appropriately provide notification under subparagraph (a), then the Responsible Party will reimburse the other party for the costs, fines, or penalties incurred as a result of its failure provide appropriate notification.

5. **Obligation to report to the other party.** Upon discovery of a Privacy Incident, Security Incident, and/or Breach, the Responsible Party will report to the other party in writing as further specified in subsection 6.2.G.

   a. **Communication with authorized representative.** Each party will send any written reports to, and communicate and coordinate as necessary with, the other party's authorized representative or designee.

b. **Cooperation of response.** Each party will cooperate with requests and instructions received from the other party 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.** Each party will, as soon as possible, but not later than forty-eight (48) hours after a request from the other party, provide the other party with any reports or information requested by the other party related to an investigation of a Security Incident, Privacy Incident, and/or Breach of protected information shared under this agreement.

6. **Documentation.** The Responsible Party for the incident or breach 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.J, whichever is longer. The Responsible Party for the incident or breach shall provide such documentation to the other party upon request.

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

1. **Federal Tax Information.** Each party will report all actual or suspected unauthorized Uses or Disclosures of federal tax information (FTI). FTI is information protected by Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. § 6103 and Publication 1075).

a. **Initial report.** Each party will, in writing, immediately report all actual or suspected unauthorized Uses or Disclosures of FTI to the other party. Each party will include in its initial report to the other party all information under subsections 6.2.F(1)–(4), of this Agreement that is available to the party at the time of the initial report, and provide updated reports as additional information becomes available.

b. **Final report.** The Responsible Authority will, upon completion of its investigation of and response to any actual or suspected unauthorized Uses or Disclosures of FTI, or upon the other party's request in accordance with subsection 6.2(F)(5), promptly submit a written report to the other party documenting all actions taken under subsections 6.2.F(1)–(4), of this Agreement.

2. **Social Security Administration Data.** Each party 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.** Each party will, in writing, immediately report all actual or suspected unauthorized Uses or Disclosures of SSA data to the other party.

Each party will include in its initial report to the other party all information under subsections 6.2.F(1)–(4), of this Agreement that is available to the party at the time of the initial report, and provide updated reports as additional information becomes available.

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

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

a. **Reporting Breaches to DHS.** MNsure will report, in writing, any Breach involving Protected Health Information to DHS 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 the individuals whose unsecured Protected Health Information has been, or is reasonably believed by MNsure, 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 MNsure'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 MNsure 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.** The Responsible Party will report all Breaches involving Protected Health Information to 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 500 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, the Responsible Party will provide to the other 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.** Each party will report, in writing, to the other party all Security Incidents that do not result in a Breach, but involve systems maintaining Protected Health Information shared pursuant to this Agreement within (5) business days of discovery. As a business associate, MNsure and its agents will comply with the applicable requirements of 45 C.F.R. § 164.314, “Organizational Requirements.”

d. **Reporting other violations.** Each party will report, in writing, to the other party any other Privacy Incident and/or violation of an Individual’s privacy rights as it pertains to Protected Health Information shared pursuant to this Agreement 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.** Each Responsible Party will report all other Privacy Incidents and/or Security Incidents, to the other party.

a. **Initial report.** The Responsible Party will report all other Privacy Incidents and/or Security Incidents to the other party, in writing, within five (5) calendar days of discovery. If the Responsible Party 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 the Responsible Party will provide the other party with all information under subsections 6.2.F(1)–(4), of this Agreement that are available to the Responsible Party at the time of the initial report, and provide updated reports as additional information becomes available.

b. **Final report.** The Responsible Party will, upon completion of its investigation of and response to a Privacy Incident, Security Incident, and/or Breach, or upon the other party’s request in accordance with subsection 6.2.E(5) submit in writing a report to the other party documenting all actions taken under subsections 6.2.F(1)–(4), of this Agreement.

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

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.

I. **Access to Books and Records, Security Audits, and Remediation.** Each party 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. Each party 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 a party. Each party 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, Minnesota Statutes, section 13.37, “General Nonpublic Data,” subd. 1(a) and 2(a).

3. Each party agrees to make its internal practices, books, audits, and records related to its obligations under the Agreement available to the other party or a designee upon the other party’s request for purposes of conducting a financial or security audit, investigation, or assessment, or to determine MNsure’s or DHS’ 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. Each party will make and document best efforts to remediate any control deficiencies identified during the course of its own audit(s), or upon request by the other party or other authorized government official(s), in a commercially reasonable timeframe.

J. **Documentation Required.** Any documentation required by this Agreement, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by a party, or of other matters pertinent to the execution of the Agreement, must be securely maintained and retained by a party 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.

Each party shall document Disclosures of Protected Health Information that are subject to the accounting of disclosure requirement described in 45 C.F.R. 164.528, “Accounting of Disclosures of Protected Health Information.”

K. **Requests for Disclosure of Protected Information.** If a party or one of its Agents receives a request to Disclose Protected Information, the party shall inform the other party of the request and coordinate the appropriate response with the other party. If a party Discloses Protected Information after coordination of a response with the other party, 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 the other party.

L. **Conflicting Provisions.** Both parties shall comply with all Applicable Safeguards listed in Section 6.1, including applicable provisions of HIPAA, and with this Agreement. To extent that the parties determine, following consultation, that the terms of this Agreement are less stringent than the Applicable Safeguards, both parties must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, each party must comply with the most stringent Applicable Safeguard.

M. **Data Availability.** Either party, or any entity with legal control of any Protected

Information provided by the other party, shall make any and all Protected Information under the Agreement available to the other party upon request within a reasonable time as is necessary for the other party to comply with applicable law.

6.3 Data Security.

A. State Information Management System Access. If a party grants the other party access to Protected Information maintained in a party's information management system (including a "legacy" system) or in any other application, computer, or storage device of any kind, then the party agrees to comply with any additional system- or application-specific requirements as directed by the other party.

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,"

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 MNsure Permitted Uses and Responsibilities regarding Protected Health Information.

A. Management and Administration. Except as otherwise limited in the Agreement, MNsure may:

1. Use Protected Health Information for the proper management and administration of MNsure or to carry out the legal responsibilities of MNsure.
2. Disclose Protected Health Information for the proper management and administration of MNsure, 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 DHS or the Disclosure is otherwise authorized by DHS, and MNsure:
      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 MNsure 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 MNsure's duties and responsibilities require it, on behalf of DHS, to obtain individually identifiable health information from Individual(s), then

MNsure shall, before obtaining the information, confer with DHS to ensure that any required Notice of Privacy Practices includes the appropriate terms and provisions.

C. **De-identify Protected Health Information.** MNsure may use Protected Health Information to create de-identified Protected Health Information provided that MNsure 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 DHS and can only be Used or Disclosed by MNsure on behalf of DHS and pursuant to the Agreement or by prior written approval of DHS.

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

6.5 DHS Permitted Uses and Responsibilities regarding Protected Information

A. **Management and Administration.** Except as otherwise limited in this Agreement, DHS may:

1. Use Protected Information for the proper management and administration of DHS or on behalf of MNsure or to carry out the legal responsibilities of MNsure or DHS, provided that any access to data classified as not public data under Minnesota Statutes, section 62V.06, subd. 3, by individual agents of DHS is approved by the MNsure Board pursuant to Minnesota Statutes, section 62V.06, subd. 8.

2. Disclose Protected Information for the proper management and administration of DHS or on behalf of MNsure, 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 MNsure or the disclosure is otherwise authorized by MNsure, and DHS:

        i. Obtains reasonable assurances, in the form of a data sharing agreement, from the entity to whom the Protected Information will be disclosed that the Protected Information will be safeguarded in accordance with law and will not be used or disclosed other than for the contracted services or the authorized purposes; and

        ii. DHS requires the entity to whom Protected Information is disclosed to notify DHS of any compromise to the confidentiality, availability, and integrity of Protected Information of which it becomes aware.

B. **Sale of Data Prohibited.** The parties are prohibited from selling any data that is classified by Minnesota Statutes, section 62V.06.

6.6 Obligations 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 the other party, each party shall immediately destroy or sanitize (permanently de-identify without the possibility of re-identification), or return in a secure manner to the other party all Protected Information that it still maintains.

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

C. In the event that a party 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 the other party 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, the party 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 the party or its Agents.

D. Each party shall document and verify in a written report to the other party 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 the other party; and

3. The identity of organization name (if different than the party), 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 the other party.

F. Any costs incurred by a party in fulfilling its obligations under this Section will be the sole responsibility of the party.

7. **LIABILITY.**

The parties agree that each is independently responsible for complying with statutes, rules, and regulations governing or affecting the collection, storage, use, sharing, disclosure, and dissemination of Protected Information in accordance with Clause 6 Information Privacy and Security. Neither party will be liable for any violation of any provision of applicable laws or the terms of this Agreement indirectly or directly arising out of, resulting from, or in any manner attributable to actions of the other party or its employees or agents. The liability of each party is governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, section 3.736, and other applicable law.

The parties acknowledge that if a party is in violation of this Agreement, or violation of a federal or state statute applicable to Protected Information, the other party may limit, suspend, or terminate the violating party's access to or use of Protected Information.

8. SEVERABILITY.

If any provision of this Agreement is held unenforceable, then such provision will be modified to reflect the parties' intention. All remaining provisions of this Agreement shall remain in full force and effect.

9. INTERPRETATION

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

10. SURVIVAL OF TERMS.

The rights and obligations of the parties under this Agreement shall survive the termination of this Agreement for as long as each party or its subcontractors and agents are in possession of Protected Information received from or collected, created, used, maintained, or disclosed on behalf of the other party. The duties and obligations of both parties in section 6.6 shall survive termination of this Agreement.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.

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

APPROVED:

1. **MNSURE**

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

DocuSigned by:
Nathan Clark
60CA7E6941CA4DB...

By: Click here to enter text

Printed Name: Nathan Clark

Title: Chief Executive Officer

Date: Click here to enter text 12/31/2020

2. **Department of Human Services (DHS)**

DocuSigned by:
E336517A7B0D415...

By (with delegated authority): Click here to enter text

Printed Name: Click here to enter text Charles E. Johnson

Title: Click here to enter text Deputy Commissioner

Date: Click here to enter text 12/31/2020

Distribution: (copy of fully executed contract to each)

Contracting and Legal Compliance Division

MNsure

DHS Authorized Representative