Amended MNsure Data Sharing Agreement

This Data Sharing Agreement ("Agreement") is by and between the Minnesota Insurance Marketplace a/k/a MNsure ("MNsure") and the Office of MN.IT Services ("MN.IT").

WHEREAS, MN.IT provides information technology services, management, and security to state agencies pursuant to Minnesota Statutes, Chapter 16E, and the parties will enter into a Service Level Agreement as to those responsibilities.

WHEREAS, MNsure is subject to the Minnesota Government Data Practices Act by Minnesota Statutes, section 62V.06, subdivision 1.

WHEREAS, MNsure and MN.IT are authorized to enter into this Agreement by Minnesota Statutes, section 62V.05, subdivision 1(b)(5) and by Minnesota Statutes, section 471.59, subdivision 10.

WHEREAS, the parties' data sharing agreement executed on June 26, 2013, is hereby amended to make changes to the privacy and security of federal tax information.

Agreement

1. Term of Agreement

1.1 ***Effective date:*** July 1, 2013, or the date the State obtains all required signatures, whichever is later.

1.2 ***Expiration date***: June 30, 2015, or until all obligations have been satisfactorily fulfilled, or until any applicable statutory authority expires, whichever comes first.

2. Information Covered by this Agreement

2.1 Under this Agreement, MNsure will be sharing with MN.IT one or more types of private information, collectively referred to as "protected information," concerning individuals, employers, and/or employees participating in MNsure. "Protected information," for purposes of this Agreement, may include any or all of the following:

2.1.1 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 governed by other sections in the Minnesota Government Data Practices Act (MGDPA), Minn. Stat. Chapter 13;

2.1.2 Protected health information ("PHI") (as defined in and governed by the Health Insurance Portability Accountability Act ("HIPAA"), 45 C.F.R. § 160.103);

2.1.3 Federal Tax Information ("FTI") (as defined by IRC § 6103);

2.1.4 Records (as defined by the Privacy Act of 1974, 5 U.S.C. § 552a); and

2.1.5 Other data subject to applicable State and federal statutes, rules, and regulations affecting the collection, storage, use, or dissemination of private or confidential information.

3. Duties

3.1 MNsure Duties. MNsure shall:

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

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

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

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

(e) Comply with all MN.IT information security policies and standards as applicable to MNsure in accordance with Minnesota Statutes section 16E.03, subdivision 7.

(f) Identify the classification of any data shared with MN.IT, and specify any applicable laws, rules, and regulations and any unique handling requirements.

(g) Notify MN.IT of any future amendments to the Final Exchange Privacy Rule at 45 C.F.R. §155.260, or any amendments to other applicable laws, rules, or regulations.

3.2 MN.IT Duties. MN.IT shall:

(a) Be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of protected information collected, created, used, maintained, or disclosed on behalf of MNsure. This responsibility includes ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed above in paragraph 2, and having implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentially, integrity, and availability of any electronic protected health information at rest and in transit that it creates, receives, maintains, or transmits on behalf of MNsure.

(b) Comply with the minimum "necessary" access and disclosure rule set forth in the MGDPA. The collection, creation, use, maintenance, and disclosure of protected information shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government. Minn. Stat. § 13.05 subd. 3.

(c) Report to MNsure any privacy or security incident regarding the information of which it becomes aware. For purposes of this Agreement, "Security incident" means the unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Privacy incident" means violation of the Minnesota Government Data Practices Act (MGDPA) and/or including, but not limited to, improper and/or unauthorized use or disclosure of Protected information, and incidents in which the confidentiality of the information maintained by it has been breached. This report must be made in writing and

submitted to MNsure immediately and in no case more than 7 days after learning of such incident.

(d) Unless provided for otherwise in this Agreement, if MN.IT receives a request to release the information referred to in paragraph 2, MN.IT must promptly notify MNsure. MNsure will give MN.IT instructions concerning the release of the data to the requesting party before the data is released.

(e) Not use or further disclose protected information created, collected, received, stored, used, maintained, or disseminated in the course or performance of this Agreement other than as permitted or required by this Agreement or as required by law, either during the period of this Agreement or hereafter.

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

(g) To the extent that any protected information is PHI:

1. Comply with the minimum necessary rule and limit the collection, creation, use, maintenance, and disclosure of PHI to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." See 45 C.F.R. §§ 164.502(b) and 164.514(d).
2. Report any breach or security incident pursuant to the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E). This report must be in writing and sent to MNsure not more than 7 days after learning of such non-permitted use or disclosure. Such a report will at least:
   (A) Identify the nature of the non-permitted use or disclosure;
   (B) Identify the PHI used or disclosed;
   (C) Identify who made the non-permitted use or disclosure and who received the non-permitted or violating disclosure;
   (D) Identify what corrective action was taken or will be taken to prevent further non-permitted uses or disclosures;
   (E) Identify what was done or will be done to mitigate any deleterious effect of the non-permitted use or disclosure; and
   (F) Provide such other information, including any written documentation, as MNsure may reasonably request.
3. Document disclosures of PHI and information related to such disclosures as would be required for MNsure to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.
4. To the extent that MN.IT uses or discloses PHI to provide health care-related administrative services on behalf of MNsure and is a "Business Associate" as defined by HIPAA, MN.IT further agrees to:
   (A) Make available PHI in accordance with 45 C.F.R. § 164.524.
   (B) Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526.
   (C) Comply with the limited disclosure rules set forth in the HITECH Act, HIPAA, and the MGDPA. To the extent possible, disclosures should be in a limited data set, which is largely information with the patients' identifying information removed, "to the extent practicable." Pertinent identifiers include, name and social security number; street address, e-mail address, telephone and fax numbers;

certificate/license numbers; vehicle identifiers and serial numbers; URLs and IP addresses; full face photos and any other comparable images; or medical record numbers, health plan beneficiary numbers, and other account numbers. If a limited data set is not feasible, or does not meet the use or disclosure, minimum necessary should be applied. The collection, creation, use, maintenance, and disclosure of protected information shall be limited to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." See, respectively, 45 C.F.R. § 164.514, 45 C.F.R. §§ 164.502(b) and 164.514(d), and Minn. Stat. § 13.05 subd. 3.

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

(E) Comply with any and all other applicable provisions of the HIPAA Privacy Rule, Administrative, and Security Standards, including future amendments thereto. In accordance with Minnesota Statutes chapter 16E.03, subdivision 7, develop written policies and procedures for safeguarding and securing PHI and complying with HIPAA and the HITECH Act, and other privacy laws.

(F) Designate a privacy official to be responsible for the development and implementation of its policies and procedures as required by 45 C.F.R. Part 164, Subpart E.

(h) To the extent that any MNsure Protected information is FTI, ensure that the FTI is only 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, Exhibit 7, and restrict from use for any other purpose.

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

(j) Comply with any and all other applicable provisions of the Final Exchange Privacy Rule at 45 C.F.R. § 155.260, including future amendments thereto.

(k) To the extent MN.IT refers data requestors to MNsure for response and makes the requested data available to MNsure for redacting and fulfilling the response, MN.IT will not be in breach of section 3.2(d) & (g)(4)(A-C) of this Agreement.

4. **Disposition of Data upon Completion, Expiration, or Agreement Termination.** Upon completion, expiration, or termination of this Agreement, and in the absence of a new data sharing agreement, MN.IT will return to MNsure or destroy all Protected information received or created on behalf of MNsure for purposes associated with this Agreement. A written certification of destruction or return to the MNsure Authorized Representative is required. MN.IT will retain no copies of such Protected information, provided that if both parties agree that such return or destruction is not feasible, or if MN.IT is required by the applicable regulation, rule or statutory retention schedule to retain beyond the life of this Agreement, MN.IT will extend the protections of this Agreement to the Protected

information and refrain from further use or disclosure of such information, except for those purposes that make return or destruction infeasible, for as long as MN.IT maintains the information.

5. Amendments

Any amendment to this Agreement must be in writing and will not be effective until it has been executed and approved by the same parties who executed and approved the original Agreement, or their successors in office.

6. Liability

The parties agree that each is independently responsible for complying with statutes, rules, and/or regulations governing or affecting the collection, storage, use, sharing, disclosure, and dissemination of protected information in accordance with this Agreement. 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 state agencies is governed by the provisions of the Minnesota Tort Claims Act, Minnesota Statutes, Section 3.736, and other applicable law.

7. Sanctions.

In addition to any liability under section 6 of this Agreement, the parties acknowledge that violation of the laws and protections described above could result in limitations being placed on future access to Protected information, in investigation and imposition of sanctions by the U.S. Department of Health and Human Services, Office for Civil Rights, and/or in civil and criminal penalties.

8. Termination

Either party may terminate this Agreement at any time, with or without cause, upon 30 days' written notice to the other party.

1. Office of MN.IT Services

By: _____
(With delegated authority)

Title: _____

Date: _____

2. Minnesota Insurance Marketplace

By: _____
(With delegated authority)

Title: MNsure Executive Director

Date: 8-15-13

The agency should include the Exhibit 7 language for either General Services or Technology Services, as appropriate and include the language below to the greatest extent possible, applicable to the specific situation.

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of

unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS:

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.