



## Data Privacy and Security Standards MNsire Consumer Assistance Partners

MNsire contains information that is personal, private and protected. You are responsible for protecting consumer privacy and the security of the system. As a Consumer Assistance Partner, you may access data that is classified by law as private and/or protected, including:

- Private data (as defined in Minnesota Statutes § 13.02, subd. 12), confidential data (as defined in Minn. Stat. § 13.02, subd. 3), welfare data (as governed by Minn. Stat. § 13.46), medical data (as governed by Minn. Stat. § 13.384), and other not public data governed by other sections in the Minnesota Government Data Practices Act (MGDPA), Minn. Stats. Chapter 13;
- Protected health information (“PHI”) (as defined in and governed by the Health Insurance Portability Accountability Act (“HIPAA”), 45 C.F.R. § 160.103);
- Federal Tax Information (“FTI”) (as defined by IRC § 6103);
- Records (as defined by the Privacy Act of 1974, 5 U.S.C. § 552a; and
- Other data subject to applicable State and federal statutes, rules, and regulations affecting the collection, storage, use or dissemination of private or confidential information.

The Minnesota Government Practices Act (MGDPA) is a Minnesota law that regulates the collection and use of personal information by state government entities and their employees and agents. Minnesota Statutes, Chapter 13. Under MGDPA, all data created, used, collected or disseminated by a government entity is presumed to be public. Personal information collected by a government entity or its employees or agents is generally classified as private data and may only be accessed to the extent necessary to do your job and may not be disclosed to anyone besides the consumer without the consumer’s consent or authorization.

In your work with MNsure, you will likely be required to protect protected health information as outlined in Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology Economic and Clinical Health Act (HITECH). The fact that a consumer has health insurance is protected health information. This information may not be shared or accessed by anyone who does not have a specific business need or authorization from the consumer.

MNsire is also subject to the 45 C.F.R. 155.260, which outlines rights of participants in MNsure to the privacy and security of their personal information. Consumers have the following rights:

- Individual access to information;
- Opportunity for correction and protection of data integrity;
- Transparent policies and choice about how information will be used;
- Safeguards and accountability; and
- Limitations on the use of data collected for MNsure to carry out MNsure functions only.



## Information Security Safeguards

MNsure may only release information that it is authorized by law or regulation to share with the Consumer Assistance Partner. Please review the MNsure Broker Certification Guidebook or your MNsure Navigator or Certified Application Counselor organizational contract for specific information about obtaining consent and any limitations on disclosure of participant data.

MNsure Consumer Assistance partners are responsible to ensure proper handling and safeguarding by employees, subcontractors, and authorized agents of protected information collected, created, used, maintained or disclosed on behalf of MNsure. This responsibility includes actions such as screening and monitoring employees to protect information privacy, training and implementing administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any protected information at rest and in transit that it creates, receives, maintains or transmits on behalf of MNsure. This includes employing appropriate storage and destruction methods to prevent the release of protected information.

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. Minnesota Statutes section 13.05 subdivision 3. Unauthorized access may subject you to civil or criminal penalties.

Consumer assistance partners are required to report to MNsure any privacy or security incident regarding MNsure information of which it becomes aware, 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 2 days after learning of such incident.

In accordance with Minnesota Statutes § 62V.06, subdivision 9, MNsure partners may not sell any data collected, created, or maintained by MNsure, regardless of its classification, for commercial or any other purposes.

Consumer assistance partners are also required to report and mitigate any fraudulent activities. Be aware of any suspicious or fraudulent activity and report to:  
[mnsurecompliancehotline@mnsure.org](mailto:mnsurecompliancehotline@mnsure.org).

MNsure partners may be subject to an audit or investigation of data security practices by authorized law enforcement or compliance personnel.



## Rules of Behavior for MNsure Employees and Contractors

The MNsure system is the property of the State of Minnesota and is subject to the Minnesota Government Data Practices Act. By using the MNsure system and data, you are representing yourself as an authorized user, and as such, you agree to use for authorized purposes only and in compliance with state and federal law. Users of the system who have the ability to see the personal information of participants, including state employees, contractors, Consumer assistance partners, and other system users, must adhere to rules of behavior for protection of private participant information. These rules are consistent with and in addition to state and federal laws and the privacy and security policies and procedures for MNsure, including the Minnesota Department of Human Services (DHS) Information and Technology Policies and Procedures, and the Appropriate Use of Electronic Communication and Technology Policy (applicable only to state employee users). Non-compliance with the rules and associated security policies may be cause for disciplinary actions including suspension and/or termination of access privileges, employment consequences, and/or civil and criminal legal action.

### **1. System Use**

System use must comply with MNsure policies and standards, and with applicable state and federal laws.

### **2. Unauthorized Access Prohibited**

Unauthorized access to the MNsure application system or use of the system for other than official, assigned duties is strictly prohibited. This prohibition includes access in excess of the minimum necessary to perform assigned job duties and training level.

### **3. Monitoring**

System and equipment use are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

### **4. Users Duty**

Users have a duty to ensure the accuracy, relevance, timeliness and completeness of personally identifiable information, as is reasonably necessary, to assure fairness in making determinations about an individual.

### **5. Authorized Purposes Only**

Privileged users may only use personally identifiable information for the purpose for which it was authorized to be collected and used.

### **6. Security Obligations**

Users have an obligation to protect the system and information from unauthorized access, use, modification, destruction, theft or disclosure by maintaining security and control over devices accessing the system, refraining from sharing account information, and using secure methods of access, storage and transmission of system information.



### **7. Incident Reporting**

Users must immediately report any lost or stolen equipment, known or suspected security incidents or breaches, known or suspected policy violations, or suspicious activity in accordance with established procedures. Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password or sensitive information maintained or in possession of MNSure or information processed by contractors and third parties on behalf of MNSure.

### **8. Disclosures**

Users shall not disclose or disseminate personally identifiable information except as authorized by law and consistent with assigned duties or with the consent of the subject of the data, where applicable.

### **9. Data Integrity**

Users may not knowingly or willingly conceal, remove, mutilate, obliterate, falsify or destroy information outside of appropriate retention periods.