



MNsure[®]

Where you choose health coverage

MNsure Privacy Program Strategic Plan 2022-2023

July 2021



Table of Contents

MNsure Privacy Program Strategic Plan 2022-2023.....	1
Table of Contents.....	2
Introduction.....	3
Privacy Program Mission.....	4
Strategic Goals of the Privacy Office.....	4
Two-Year Goals.....	4
Long-Term Goals.....	6
Privacy Office Operations.....	6
Key Focus Areas.....	6
Staff Resources.....	6
Other Stakeholders.....	7
Privacy Office Performance Metrics.....	8
Annual Approval Process.....	9
Biannual Approval Procedures:.....	9
Approved by:.....	9
Revision History.....	9

Introduction

The purpose of this Privacy Program Strategic Plan (“the Plan” or “the Privacy Plan”) is to outline MNSure’s Privacy Office’s mission and vision. The Privacy Plan outlines the goals, functions and procedures of the Privacy Office that are incorporated into MNSure’s Privacy Program. While the Privacy Office has been in place at MNSure since 2013, MNSure has developed this Plan to better document and communicate the direction and efforts of the Privacy Office.

Throughout the Plan there are references to the “Privacy Program” and the “Privacy Office.” “Privacy Program” describes the sum of all efforts and activities related to privacy throughout the organization, while the Privacy Office describes the business unit tasked with advising, supporting and guiding the organization’s efforts and activities related to data privacy. This distinction is important because, like compliance, protecting not public data is the responsibility of all MNSure staff members.

The Privacy Office is one of several business functions that report to MNSure’s General Counsel (“General Counsel”). In particular, the Privacy Office works closely with the Compliance Department to foster staff awareness of regulatory requirements and works to ensure that staff have the knowledge and tools available to remain compliant. Though the Privacy Office and Compliance Department are separate units at MNSure, they work closely together to emphasize the importance of privacy compliance.

As separate business units, the Privacy Office and Compliance Department each have their own separate strategic plans (the “Compliance Plan” and the “Privacy Plan”). In some cases, the plans may have coinciding goals, and staff from both areas will work together to achieve those goals.

The Privacy Plan’s activities are organized into the following key focus areas, consistent with other well-regarded privacy programs and available guidance from across the U.S.:

1. Oversight and Responsibility
2. Risk Assessment and Monitoring
3. Safeguards (Physical, Administrative)
4. IT Security and Technical Safeguards
5. Policies and Procedures
6. Training
7. Individual Privacy Rights
8. Response, Mitigation and Prevention

Privacy Program Mission

In light of the Compliance Department's and Privacy Program's intersecting goals, the Privacy Office has adopted the Compliance Department's mission. Notably, all members of MNSure are responsible for carrying out compliance, which includes compliance with data practices and privacy laws.

MNSure views compliance as a responsibility of all employees throughout the organization and will implement the appropriate systems and structures to provide all employees and business units support, advice and guidance to assure ethical and regulatory requirements are identified and met.

MNSure shall operate as an ethical, compliant and transparent organization by fostering a culture of honesty and accountability, while adhering to the regulatory requirements governing our organization. Additionally, MNSure views compliance as the responsibility of all employees in order to help us achieve our mission to ensure all Minnesotans have the security of health insurance.

Strategic Goals of the Privacy Office

The following key strategic goals of the Privacy Office are high-level goals that will guide the Privacy Office beyond its day-to-day activities and functions. These goals are intended to help enhance MNSure's overall Privacy Program. These goals will focus on implementing and maintaining the appropriate infrastructure to allow the Privacy Office to fulfill its mission.

Objective: Strengthen the crucial infrastructure needed for MNSure's privacy program.

Strategy: The Privacy Office will develop a detailed action or work plan outlining the steps necessary to achieve the goals listed below.

Measurement: Progress with the developed work plan will be tracked to help ensure timelines are met. Success will be defined by having the associated deliverables or processes developed or implemented by June 30, 2023.

Accountability: David Rowley, General Counsel and Chief Compliance Officer

Reporting: Progress and status reports will be given to the Executive Team and the MNSure Board of Directors' Compliance Workgroup quarterly.

Two-Year Goals

By June 30, 2023, complete these tasks assigned to each of the following key focus areas:

Oversight and Responsibility

- Report high-level metrics regarding privacy training, privacy incidents and audit findings to the MNSure Executive team and the MNSure Board of Directors' Compliance Workgroup, as appropriate

Risk Assessment and Monitoring

- Conduct an annual privacy risk assessment
- Implement a program to monitor MNsure's third party vendors in conjunction with the Compliance Department
- Implement methods to monitor METS' audit log data in conjunction with the Compliance Department

Administrative and Physical Safeguards

- Annually update MNsure's data sharing agreement template to reflect changes in MNsure's operations or applicable law
- Inventory and track all data sharing agreements
- Annually review staff members' access to applications and locations with not public data to ensure access remains appropriate

IT Security and Technical Safeguards

- Incorporate MNIT Enterprise security policies and standards into MNsure administrative privacy policies
- In conjunction with MNIT staff, complete annual attestation for federal Centers for Medicare and Medicaid Services (CMS) to evaluate compliance with federal standards
- Annually review the MNsure Security Scorecard prepared by MNIT with MNIT staff, including updating the inventory of applications being used by MNsure staff

Policies and Procedures

- Review and update MNsure's administrative policies and procedures regarding privacy
- Annually update MNsure's data inventory
- Develop and share regular communications or training to increase awareness of MNsure's privacy policies and procedures

Training

- Develop targeted privacy training for business units
- Incorporate and maintain IT security controls in annual training

Individual Privacy Rights

- Annually review MNsure's Tennessee warnings and data collection practices to ensure data is only used for the purpose for which it was collected
- Complete the annual Privacy Impact Assessment as required by CMS

Response, Mitigation and Prevention

- Implement controls to mitigate risks identified after a privacy or security incident

Long-Term Goals

1. MNsure's Privacy Office will have established processes and procedures to protect private information that are consistent and tested. The long-term goal is that this infrastructure will be operating effectively.

Accountability: David Rowley, General Counsel and Chief Compliance Officer

2. Create privacy competence throughout MNsure through continuous education and in conversations with the Executive Team.

Accountability: David Rowley, General Counsel and Chief Compliance Officer

Privacy Office Operations

This section focuses on the ongoing operations of the Privacy Office. It outlines the Privacy Office's key focus areas, organizational structure and staff resources. Finally, this section defines the metrics used to measure the effectiveness of the Privacy Office.

Key Focus Areas

MNsure's Privacy Office's core focus areas are essential to ensuring the private information entrusted to MNsure is adequately safeguarded and MNsure's consumers understand their privacy rights. The key focus areas reflect the day-to-day activities performed by the Privacy Office. Key focus areas include:

1. Oversight and Responsibility
2. Risk Assessment and Monitoring
3. Safeguards (Physical, Administrative)
4. IT Security and Technical Safeguards
5. Policies and Procedures
6. Training
7. Individual Privacy Rights
8. Response, Mitigation and Prevention

Staff Resources

Appropriate staffing of the Privacy Office assures that MNsure will achieve its privacy compliance mission.

Privacy and Security Officer

The Privacy and Security officer is responsible for development, implementation, delivery, maintenance and adherence to a comprehensive information privacy and security program for MNsure. The MNsure Privacy and Security officer ensures that information created, acquired or maintained by MNsure and its authorized users is used in accordance with its intended purposes and works to ensure that MNsure complies with privacy and security statutory, regulatory and policy requirements.

The Privacy and Security officer must:

- Develop and articulate a clear strategic vision of privacy compliance for MNsure.
- Communicate with senior leadership on privacy and security risks and controls.
- Establish effective working relationships and build credibility within the organization and among its external stakeholders.
- Collaborate with stakeholders on privacy and security issues and appropriate controls.
- Establish and maintain a privacy and security training plan to foster awareness and compliance with privacy laws and policies.
- Train new staff on MNsure privacy and security.
- Prepare thorough legal analysis on privacy and security incidents and carry out incident notifications and reporting.
- Monitor the completion of security and privacy documents submitted to federal oversight partners, like CMS.
- Conduct privacy impact assessments and risk assessments for MNsure business units.
- Provide guidance and manage the responsibilities of any staff attorney or law clerk assigned to the Privacy Office to ensure MNsure's compliance with the Minnesota Government Data Practices Act.
- Monitor the performance of the Privacy Program and related activities on a continuing basis, taking appropriate steps to improve its effectiveness.

Other Stakeholders

MNsire General Counsel and Chief Compliance Officer

The MNsure General Counsel manages the Privacy Office staffing and budget and provides guidance and oversight to ensure that the program meets organizational needs and operates in compliance with applicable law.

MNsire Chief Executive Officer

The MNsure Chief Executive Officer serves as the Responsible Authority for the collection, use and dissemination of any set of data on individuals, government data or summary data under the Minnesota Government Data Practices Act.

MNIT Security Manager

The MNIT Security Manager supervises the development, implementation and operation of the METS security program and oversees MNSure information technology security. This manager and his or her team provides advice and guidance on MNSure security risks and program enhancements.

MNSure External Relations

- The MNSure Government Affairs Manager collaborates with the Privacy Office on responding to data requests from the Minnesota Legislature and Congressional oversight bodies.
- The MNSure Director of Public Affairs collaborates with the Privacy Office on the release of public information for press releases and social media posts, and in response to requests from news outlets and reporters.
- The MNSure Senior Director of Public Affairs collaborates with the Privacy Office on open meeting law issues and information privacy and security document submissions to CMS and the Center for Consumer Information and Insurance Oversight (CCIIO).

MNSure Operations

Managers, directors and staff within MNSure business operations units routinely work with the Privacy Office as needed for advice and guidance on data practices, records retention and information privacy issues; for risk assessment and privacy impact analysis; and for reporting and responding to privacy incidents, breaches and investigations.

Privacy Office Performance Metrics

The Privacy Office has developed performance metrics as a quantitative measurement of its work. These metrics are intended to drive the Privacy Office towards achieving its mission. Progress on the metrics will be reported to the MNSure Executive Team and the MNSure Board of Directors' Compliance Workgroup on at least a quarterly basis. The performance metrics must be re-visited annually and adjusted as necessary.

The 2022-2023 performance metrics are as follows:

- Ensure 100% of employees complete the annual privacy and security training by November 1 each year.
- Conduct a privacy risk assessment and report to the MNSure Board of Directors' Compliance Workgroup by July 31 each year.
- Provide each new employee with in-person privacy training within one week of the employee's appointment.
- Provide privacy or security updates or reminders to all staff at least monthly.

- Complete an audit of staff access to one of MNsure’s high-risk applications (METS, CRM, FileNet, etc.) at least quarterly to ensure each staff member has appropriate access given their training and role.

Annual Approval Process

The Privacy Plan should be reviewed, updated and approved by the MNsure Board of Directors annually in conjunction with the Compliance Plan.

Biannual Approval Procedures:

1. Biannually, the Chief Compliance Officer must review update and submit the Privacy Strategic Plan to the MNsure Executive Team for review.
2. Once approved by the Executive Team, the plan will be submitted to the MNsure Board of Directors for approval.
3. The Privacy Plan should be tracked with:
 - a. Dates of revision
 - b. Revision/editor information
 - c. Signature of the MNsure Board of Directors chair

Approved by:

Name:

Title: Chair, MNsure Board of Directors (signing on behalf of the board)

DocuSigned by:

 Signature: _____

7/26/2021
 Date: _____

Revision History

Version	Editor	Date
Original	Lindsey Millard	May 15, 2018
Version 2	Lindsey Millard	June 1, 2019
Version 3	Emily Cleveland	June 1, 2021