



## **MNsure Privacy Program Strategic Plan FY 2018-2019**

July 2018

## Table of Contents

Introduction .....	3
Privacy Program Mission .....	4
Strategic Goals of the Privacy Office.....	4
Short-Term Goals .....	4
Long-Term Goals .....	6
Privacy Office Operations .....	6
Key Focus Areas.....	6
Staff Resources .....	6
Privacy Office Performance Metrics .....	9
Annual Approval Process.....	10
Annual Approval Procedures:.....	10
Revision History .....	10

## Introduction

The purpose of this Privacy Program Strategic Plan (“the Plan” or “the Privacy Plan”) is to outline the Privacy Office’s mission and vision. The Privacy Plan also 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 increase awareness of the direction and efforts of the Privacy Office.

Throughout the Plan there are references to the “Privacy Program” and the “Privacy Office.” “Privacy Plan” 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 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 and Privacy Programs' intersecting goals, the Privacy Office has adopted the Compliance Program's mission. Notably, all members of MNsure are responsible for carrying out compliance, which includes compliance with data practices and privacy laws.

*MNsire 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.*

*MNsire 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 the appropriate infrastructure to allow the Privacy Office to fulfill its mission.

### Short-Term Goals

*By June 30, 2019, complete the tasks assigned to the following key focus areas:*

#### Oversight and Responsibility

- Develop a privacy dashboard to report high-level metrics regarding privacy training, privacy incidents, and audit findings to the MNsure Executive team and the MNsure board's Compliance Workgroup, as appropriate

#### Risk Assessment and Monitoring

- Conduct an annual privacy risk assessment
- Implement a third-party monitoring program in conjunction with the Compliance Department
- Request periodic audits from the Compliance Department to monitor compliance with privacy controls and identify risks

#### Administrative and Physical Safeguards

- Review and update MNsure's data sharing agreement template to reflect changes in MNsure's operations or applicable law

- 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 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**

- Inventory, review, and update MNsure's administrative policies and procedures regarding privacy
- Develop disciplinary standards for privacy policy or procedure non-compliance

## **Training**

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

## **Individual Privacy Rights**

- Annually review MNsure's Tennessen 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
- Develop and implement a non-retaliation policy for privacy complaints

## **Response, Mitigation and Prevention**

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

**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 above.

**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 and or processes developed by June 30, 2019.

**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 Compliance Workgroup quarterly.

## 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 on-going 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

The 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 the MNsure will achieve its privacy compliance mission.

### Privacy and Security Manager

The Privacy and Security manager is responsible for the development, implementation, delivery, maintenance, and adherence to a comprehensive information privacy and security program for

MNsure. The MNsure Privacy and Security Manager 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 Manager 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 the Staff Attorney 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.

### **Staff Attorney and Data Practices Coordinator**

The Staff Attorney is responsible for providing training and guidance to MNsure to ensure its compliance with the Minnesota Government Data Practices Act.

The Staff Attorney must:

- Plan and coordinate data practices training for MNsure staff and contractors and update MNsure data practices training materials.
- Provide consistent, timely, accurate, and legally sufficient responses to requests for data in accordance with the Minnesota Government Data Practices Act.
- Establish and maintain a records retention program and communicate the records retention schedule to MNsure business units.
- Maintain continuing knowledge and expertise of electronic data storage and emerging technologies for records management.

- Provide legal analysis and guidance on data practices and privacy issues.
- Manage agency legal holds in coordination with the Privacy and Security Manager and the MNsure General Counsel.
- Communicate with MNsure External Affairs on data practices requests and issues related to media and legislative inquiries.

## **Other Stakeholders**

### ***MNsure 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.

### ***MNsure 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 Relations 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, social media posts, and in response to requests from news outlets and reporters.
- The MNsure Board and Federal Relations Director collaborates with the Privacy Office on open meeting law issues and CMS/CCIIO information privacy and security document submissions.

### ***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 Compliance Workgroup on at least a quarterly basis. The performance metrics must be revisited annually and adjusted as necessary.

The fiscal year 2018-2019 performance metrics are as follows:

- Ensure 100 percent of employees complete the annual privacy and security training by November 1, 2018.
- Conduct a privacy risk assessment and report to the MNsure Board Compliance Workgroup by July 31, 2019.
- 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.

### Annual Approval Procedures:

1. Annually, 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 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 Chairperson

### Approved by:

Name: Phil Norrgard

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

Signature:



Date: July 18, 2018

## Revision History

Version	Editor	Date
Original	Lindsey Millard	May 15, 2018