TO: April Todd-Malmlov, Executive Director

FROM: Michael Turpin, General Counsel

DATE: September 19, 2013

RE: Broker Roster Email – Incident Response Details

On September 12, 2013, MNsure was notified that an email containing MNsure's broker roster was inadvertently sent to a broker interested in partnering with MNsure. The roster contained personal information, including names, addresses, license numbers and social security numbers, on brokers who filed a notice of intent to partner with MNsure. Immediately upon notification, MNsure activated its incident response procedures. MNsure staff immediately followed up with the recipient of the email and confirmed that the email was deleted and was not further disseminated or its contents further disclosed. MNsure obtained written confirmation that the recipient of the email had not sought to receive this data, that the data was not further disseminated, and that the data was deleted per instructions from MNsure staff. At the consent of the recipient of the email, MNsure coordinated with MN.IT Services to have MN.IT Services staff conduct an in-person analysis of the computer system of the recipient of the email to ensure that file evidence was deleted and not further disseminated.

In response to this incident, the Legal and Compliance Division has begun conducting a unit-by-unit, workstation-by-workstation data privacy and security compliance review to ensure that all appropriate policies and procedures are not only in place, but in practice. Finally, MNsure will conduct a root cause analysis to identify the factors that contributed to this incident and identify any other policies or procedures that can be implemented to prevent this type of incident from occurring in the future.

<u>Data Disseminated</u>

The email contained data on 1587 individual brokers listed on a spreadsheet. The initial report stated that the incident involved 2400 individual broker names, but several brokers were listed twice on the spreadsheet for dual broker and agency

81 East 7th Street, Suite 300 ▪ St. Paul, MN 55101-2211 ▪ mnsure.org

administrator roles. The email was not encrypted and the spreadsheet was not password-protected. The data disclosure involved the following data fields:

Last Name	Agency Name
First Name	Agency Street Address
Middle Initial	Agency City
National Producer Number (NPN)	Agency State
MN License Number	Agency Zip Code
Social Security Number	Agency Admin
Broker Phone Number	Agency Admin Email
Broker's Email Address	MNsure Role (Broker or Admin)
Employment Status (content varies – owner, VP, active, etc.)	

Data Collection and Storage

MNsure collected Social Security numbers (SSN) in its broker certification process. SSNs are used in SIRCON, which is a national source database for insurance producers, in order to enter continuing education credits and to look up licensure. As the MNsure business process was developed for broker certification, it was believed that an SSN, along with two other identifiers, were required to perform a search in SIRCON, but MNsure has subsequently learned that only one of these three identifiers are required to perform a search.

The broker roster file was located in a shared drive separate from the blank template file that was intended to be distributed to brokers for collection of the data fields. In this incident, the template and master roster files had been copied to the computer's desktop rather than accessed from the segregated file.

Timeline

MNsure's incident response procedures are time-sensitive due to potential reporting requirements to state and federal oversight agencies and data sharing partners. As such, the following events were logged as part of MNsure's incident response process:

9/12/13	10:13 AM	Email sent from MNsure employee to broker and his office assistant containing master broker list with protected data.
9/12/13	10:41 AM	Email sent from MNsure employee to broker and office assistant stating that previous message was in error and should be deleted. Message included new attachment (blank spreadsheet template).
9/12/13	10:45 AM	MNsure employee who sent the email contacted broker by phone to discuss email and to confirm that it had been deleted.
9/12/13	11:30 AM	MNsure employee who sent email reported incident to Privacy and Security Manager. Incident response procedure activated.
9/12/13	12:33 PM	MNsure Privacy and Security Manager contacted broker recipient to follow up regarding email. Broker indicated that he had opened the attachment and scanned the information. He also confirmed that he and his assistant had deleted the attachment.
9/12/13	1:17 PM	Incident Report completed and sent to General Counsel. Legal and Compliance Office conducts legal analysis and internal communications.
9/12/13	5:30 PM	MNsure General Counsel contacts recipient, and recipient agrees to allow MNsure IT resources to conduct forensic examination and data purging of computer equipment.
9/12/13	6:41 PM	MNsure Privacy and Security Manager notifies MN.IT Acting Chief Information Security Officer. Communications with MN.IT ongoing.
9/13/13	11:00 AM	Email notification to brokers.
9/13/13 – present		MNsure Contact Center fields inquiries and comments.
9/15/13	1:50 PM	Broker recipient confirms in writing that he did not solicit the information, agreed that it was an accidental transfer, and consented to forensic examination of his computer equipment.

9/16/13	9:10 AM	Email from MNsure Executive Director to all staff and consultants on data privacy and security obligations and setting up business team security reviews.
9/18/13	2:00 PM	MN.IT Services staff conduct on-site examination of computer system to ensure file and data deletion.
9/19/13	12:20 PM	Email to brokers describing updated information on incident investigation.
9/19/13		MNsure Legal and Compliance Division staff begin business unit reviews and data protection assistance.

MNsure Policies and Procedures

MNsure has policies and procedures in place regarding data security and complies with state and federal law governing the use, collection, and dissemination of personal information. MNsure has adopted the Department of Human Services Information Policies, which provide that users must exercise due care and follow the appropriate standards and procedures when handling protected information. DHS Policy 2.19.

MNsure's Administrative Policy on Data Practices outlines the Minnesota Government Data Practices Act and indicates that certain personally identifiable data on individuals is classified as private and may only be released to the subject of the data or to another with written consent from the subject of the data. To comply with minimum necessary privacy requirements, the sender of an email must ensure that all recipient(s) are the appropriate audience to receive the protected information prior to sending the email. DHS Policy 5.1.2.

MNsure established Rules of Behavior as part of its comprehensive System Security Plan, and the rules state that 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. The rules also require immediate notification of suspected breaches and responsibilities for protecting equipment and data.

The Enterprise Policy on Electronic Mail (MN.IT) requires that all outgoing email messages containing nonpublic data must be encrypted. DHS Policy further specifies that encryption must be employed when handling or transmitting protected information to external email, and staff must use only State email systems to send or received protected information. DHS Policy 5.1.2. The process and rules to be used by employees for encrypting email are contained in DHS Policy 5.1.3.

The Statewide Policy on Appropriate Use of Communication and Technology further cautions employees to use care in communicating information not meant for public viewing and to encrypt or encode any data classified as not public when transmitting through unsecured areas or over email or internet systems.

Finally, in the event of an incident, MNsure has incorporated guidance from the MN.IT Enterprise Information Security Incident Management Standard and DHS Policies 6.5 and 6.6 in adopting a process for incident response (MNsure Administrative Policy on Security Incidents and Breach Reporting). Staff are required to immediately report any suspected or known security or privacy incidents or breaches. MNsure then communicates through appropriate channels to notify the executive, legal and public relations units to coordinate incident investigation and notifications.

MNsure Staff Training

MNsure staff and contractors are required to complete courses on data privacy and security, and compliance with this requirement is monitored. The courses are entitled, "Protecting Information Security" and "Putting Security into Action." The data privacy and security courses are available online, and staff are informed of the obligation to complete them through onboarding materials, email notices from the Privacy and Security Manager, in-person reminders at staff meetings, and through the MNsure SharePoint site. Relative to this incident, the training covers the following points and assessment test subjects:

1. Protected information may not be sent via the Internet or unsecured networks unless the information is encrypted.

2. Users should store personal information and work unit information on two separate drives. The local drives are reserved for the computer's operating system and files should not be stored on the local drive.

3. Users must exercise extreme caution when sending protected information via email. The State has an encryption tool that must be used, and the training contains a step-by-step instruction guide for encrypting email.

MNsure staff, consultants, contractors and consumer assistance partners are all directed to complete privacy and security training, and MNsure has a 95% completion rate for staff as of September 19, 2013. The remaining 5% are new staff who started this week and who are expected to complete training in the first week of employment.

Post-Incident Actions

As a result of this incident, MNsure staff, consultants and contractors have heightened awareness to the rules and procedures for protection of private data. On Monday, September 16, Executive Director Todd-Malmlov issued an email notification describing the incident and setting forth specific action items for completion. It was expected that all staff complete privacy and security training if they had not already done so, and managers were instructed to provide time and resources for the completion of these courses.

Additionally, the Legal and Compliance Division has begun to conduct business unit reviews and to distribute additional security reminders including instructions on technology tools for encryption, password protection, tracking data through inventories and secure storage. Business areas are also critically evaluating the purposes for which data is collected and how it is accessed and stored. These reviews are expected to provide direct assistance for secure handling of the different types of unique data that are managed each business area.

The MNsure Contact Center continues to receive and respond to inquiries related to the incident and to provide up-to-date information on the measures taken to ensure deletion of the file that was disseminated in this matter. MNsure sent notifications to brokers in an effort to provide details about the incident and timely notification of investigative progress.

Finally, MNsure will also conduct a root cause analysis to identify factors that contributed to this incident. It is expected that through work unit reviews and the root cause analysis, MNsure will identify any other policies or procedures that can be implemented to prevent this type of incident from occurring in the future.

It is important to note that this incident was not related to the public-facing MNsure IT system and that significant technological and administrative safeguards in the IT infrastructure have been implemented and assessed by multiple independent entities. Through this incident, MNsure has identified a need to further educate employees on data protection for manual processes and the consequences of failing to adhere to MNsure's policies for the handling of protected data.

Attachments

A. MNsure Administrative Policy on Data Practices
B. MNsure Administrative Policy on Information Protection
C. MNsure Administrative Policy on Security Incident or Breach Reporting
D. MNsure Rules of Behavior
E. Statewide Policy on Appropriate Use of Communication and Technology
F. MN.IT Enterprise Security Policy on Electronic Mail
G. MN.IT Enterprise Information Security Incident Management Standard
H. DHS Policy 2.19 – Physical Handling of Protected Information
I. DHS Policy 5.1.2 – Sending and Receiving Protected Information via Email
J. DHS Policy 5.1.3 – Securely Transmitting Protected Information
K. DHS Policy 6.5 – Reporting of Suspected or Known Security or Privacy Incidents
L. DHS Policy 6.6 - Responding To and Handling Suspected or Known Incidents
M. Email Notification to Brokers (September 13, 2013)
N. Email to MNsure Staff on Data Security (September 16, 2013)
O. Email Update to Brokers (September 19, 2013)