OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

MNsure: An Unauthorized Disclosure of Private Data

Special Review

November 7, 2013 **Report 13-27**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us
Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OLA
OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

November 7, 2013

Senator Roger Reinert, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Members of the MNsure Legislative Oversight Committee

Brian Beutner, Chair
MNsure Board

April Todd-Malmlov, Executive Director
MNsure

This report presents the results of our special review of an unauthorized disclosure of private data by a MNsure employee. The employee and MNsure officials cooperated fully with our review.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Table of Contents

MNsure: An Unauthorized Disclosure of Private Data

Background

On September 12, 2013, a MNsure employee e-mailed a document with private data in it to an individual not authorized to see the data. MNsure is the state agency that manages Minnesota's health insurance exchange. The private data, including Social Security numbers, had been gathered by MNsure from insurance brokers seeking certification to use MNsure's Web site to sell insurance products.

The Office of the Legislative Auditor (OLA) learned of the unauthorized disclosure of brokers' private data on September 13, 2013, through a newspaper article.[1] Given OLA's responsibility to examine the security of private data maintained by state agencies, we decided to review the unauthorized disclosure.[2]

In conducting the review, we interviewed, under oath, the MNsure employee who made the unauthorized disclosure and the employee's immediate supervisor. We also discussed various matters related to the disclosure with MNsure officials and staff, the insurance broker who received the private data from MNsure, and representatives of insurance agents and brokers. In addition, we reviewed laws, policies, and procedures relevant to the disclosure; the data security and privacy training MNsure requires of its employees; and a memorandum MNsure's General Counsel prepared on the disclosure and MNsure's response.[3]

We reached the following conclusions:

The disclosure by a MNsure employee was unintentional; we found no evidence of malicious intent. MNsure responded appropriately after the disclosure occurred.[4]

In developing a certification process for insurance brokers, MNsure officials made decisions that contributed directly to the disclosure of private data.

[1] Jackie Crosby, "Errant e-mail creates security breach at MNsure," *StarTribune*, September 13, 2013.

[2] *Minnesota Statutes* 2013, 3.971, subd. 6a.

[3] Michael Turpin, MNsure General Counsel, memorandum to April Todd-Malmlov, MNsure Executive Director, *Broker Roster Email – Incident Response Details*, September 19, 2013.

[4] Our conclusion does not include a judgment on MNsure's decision to terminate the employee who disclosed the private data.

We based our conclusions on the findings that follow.

Conclusion

The disclosure by a MNsure employee was unintentional; we found no evidence of malicious intent. MNsure responded appropriately after the disclosure occurred.[5]

Findings

Finding 1

The unauthorized disclosure of private data occurred when a MNsure employee mistakenly attached a document containing private data to an e-mail. We found no evidence of malicious intent.

The employee was hired as a broker coordinator to assist MNsure in training, certifying, and supporting licensed insurance brokers and agents who want to sell insurance products available through MNsure. The employee started work at MNsure on August 13, 2013.

One of the employee's responsibilities was to work with brokers to obtain the information MNsure required from them to begin the training and certification process. That information was primarily gathered by e-mailing brokers an electronic spreadsheet with column headings indicating the data MNsure required. Brokers were told to complete the spreadsheet and return it as an attachment to an e-mail. A MNsure employee would then cut and paste the data into a master spreadsheet called the "MNsure Broker Data Roster."[6] Among the data MNsure required from brokers were the following:

Name
National Producer Number[7]
Minnesota License Number
Social Security Number
Agency Name, Address, Phone Number, and E-mail Address

[5] Our conclusion does not include a judgment on MNsure's decision to terminate the employee who disclosed the private data.

[6] Both the spreadsheet sent to brokers and MNsure's Broker Data Roster were developed using Microsoft Excel.

[7] The National Producer Number System was established in the mid-1990s by the National Insurance Producer Registry, a nonprofit organization affiliated with the National Association of Insurance Commissioners. The Registry maintains a national database of information about insurance agents, brokers, agencies, and adjusters, which are referred to as "insurance producers." According to the Registry, it created the National Producer Number System and assigns a number to individual insurance producers as a "solution to privacy issues surrounding the use of the Social Security number." For more information about the National Producer Number System and the Registry, go to the Registry's Web site at: http://www.nipr.com/index.html.

On September 12, the employee followed up with a broker who wanted to be certified to sell products available through MNsure. Rather than attach a blank spreadsheet for the broker to fill out, the employee attached the MNsure Broker Data Roster with data for approximately 1,500 brokers.[8]

Shortly after sending the e-mail, the employee realized the MNsure Broker Data Roster had been attached rather than a blank spreadsheet. In our interview, the employee said:

> I knew immediately the magnitude of the error. I couldn't believe it. I was—I'm still in disbelief. I don't know how—well, as I said, I didn't know I could even possibly do that. I would have never imagined that that is something I could have done. I—in my mind I thought that those types of numbers were protected so you couldn't send them out. You know, like there would be a safety that was allowed to say, nope, you can't do this. I mean, I just never even imagined it could have—I couldn't believe it could happen.

The employee told us a colleague examined the e-mail and attachment and confirmed what had occurred. In response, the employee contacted the recipient of the e-mail and the recipient's administrative assistant to request that they delete the roster from their computers. The employee also notified MNsure's data privacy officer. We will discuss how MNsure officials responded in the next finding.

We found no evidence that what occurred was anything other than a mistake, and no evidence that there was any reason the employee would have intentionally shared the MNsure Broker Data Roster with the broker who received it. We asked both the MNsure employee and the broker if they knew each other (other than from the events described in this report), and both said "no."

Finding 2

MNsure responded quickly to the unauthorized exposure of private data and followed the notice requirements of state law.

Based on the interviews we conducted and the documents we obtained, we are satisfied that MNsure staff and officials acted quickly to mitigate the impact of the unauthorized disclosure of private data. The response started with the MNsure employee who was responsible for the disclosure and was continued by various MNsure officials and staff.

[8] It was originally reported that the MNsure Broker Data Roster contained data on 2,400 brokers, but MNsure officials later indicated that the number included duplicates, and the actual number was approximately 1,500.

For example, as required by state law, MNsure's General Counsel promptly notified the brokers who had their private data disclosed.[9] The notice, which was e-mailed on September 13, 2013, told brokers what data had been disclosed. It also said that, based on MNsure's investigation of the incident, MNsure had confirmed that brokers' private data was not disseminated beyond the individual to whom it was inadvertently sent. The e-mail assured brokers "…your personal data remains private." Finally, the e-mail told brokers to contact the MNsure Contact Center if they had questions or concerns.

On October 14, 2013, MNsure's executive director sent a letter to brokers to apologize for the disclosure of their private data and announce that MNsure would pay for each broker to obtain one year of identity protection from CSID, a company MNsure characterized as "the leader provider of global, enterprise level identity protection and fraud detection solutions and technologies." MNsure also indicated to the brokers that it intends to secure "a third-party contractor to perform a root cause analysis of the incident to identify any additional measures that can be taken to prevent this type of incident from occurring in the future."[10]

In addition to interviewing MNsure staff and obtaining documents from MNsure about how the agency responded to the disclosure of private data, we also contacted the broker who received the MNsure Broker Data Roster. He confirmed that shortly after receiving the roster, he was contacted by the MNsure employee who sent it and was asked to delete the document from his computer (and the computer used by his administrative assistant).[11] In addition, the broker confirmed that, shortly thereafter, he was contacted by an individual who identified herself as MNsure's Manager of Data Privacy and Security who discussed with him how to ensure that the roster had been deleted. Finally, the broker confirmed that a staff person from the state's information systems support agency (MN.IT Services) was coming to the broker's office to examine his computers to ensure that the roster had been deleted.

Finally, we note that MNsure terminated the employee who inadvertently disclosed private data. As noted in footnotes 4 and 5, we make no judgment on the appropriateness of that decision. We simply point out in the conclusion and

[9] *Minnesota Statutes* 2013, 13.055, subd. 2. The law requires that the notice "…must be made in the most expedient time possible and without unreasonable delay…." As noted previously, OLA learned of the unauthorized disclosure of private data from a newspaper article, not from MNsure. *Minnesota Statutes* 2013, 3.972, subd. 9, requires state agencies to promptly notify the Legislative Auditor when an unauthorized disclosure of private data occurs. However, since we told MNsure we were aware of the disclosure shortly after the newspaper article appeared, we decided not to cite MNsure for noncompliance with the OLA notification requirement.

[10] Letter from April Todd-Malmlov, MNsure Executive Director, October 14, 2013.

[11] The broker told us that he was "very concerned" about having received the private data not only because he felt it showed inadequate security at MNsure but also because he feared it could expose him to liability, even though he was not responsible for having obtained the data. The broker also told us that he insisted that the MNsure employee notified a supervisor about what had occurred.

findings that follow that MNsure officials made decisions that contributed directly to the disclosure of private data.

Conclusion

In developing a certification process for insurance brokers, MNsure made decisions that contributed directly to the disclosure of private data.

Finding 3

MNsure decided to collect Social Security numbers from insurance brokers although that data was not needed for MNsure to fulfill its responsibilities.

MNsure decided to require brokers to provide the agency with their Social Security numbers in addition to two other identifying numbers—a national producer number and a Minnesota producer license number.[12] MNsure thought Social Security numbers were needed for the agency to report and access information about brokers maintained by SIRCON, a national registry of information used by the Minnesota Department of Commerce.[13]

In response to our questions about the risk associated with collecting Social Security numbers, the manager of MNsure's broker team said the following:

> …I did vet that by our data security officer, and she did ask why we were collecting Social Security numbers. And I explained that to our knowledge we needed that point of information to do the CE [continuing education] credits in SIRCON. She asked that I check with Commerce as to whether that was true. I did send that roster over to the Department of Commerce, requested that they vet the roster and let us know does this look okay. I believe a few staff looked at it over there, that they returned it, and they had some edits on the front page but no comments about the Social Security number.

We contacted SIRCON and officials at the Minnesota Department of Commerce and were told that MNsure did not need Social Security numbers to interact with SIRCON.

In addition, representatives of insurance agents and brokers told us that, before the disclosure of private data occurred, they had raised objections to MNsure requiring Social Security numbers as part of the certification process, as well as to the use of unsecured e-mail for the transmission of private data.

---

[12] For a discussion of the national producer number, see footnote 7, page 2.

[13] *SIRCON for Educational Providers* is the name of a service operated by Vertafore, a company that provides various services to the insurance industry. SIRCON is an electronic registry of information about insurance-related courses where insurance agents, brokers, etc., as well as course providers, can register continuing education credits.

We also learned that in requesting private data from brokers, MNsure failed to provide brokers with a "Tennessen Warning," a requirement in the *Minnesota Government Data Practices Act*.[14] If brokers had been given the warning, they would have known how MNsure was going to use their Social Security numbers and whether they could refuse to provide that or other private information.

Finally, we note that at a meeting of the MNsure Legislative Oversight Committee on September 24, 2013, MNsure's executive director told legislators that MNsure had determined it was not necessary for the exchange to collect Social Security numbers from brokers. However, in an interview we conducted on September 27, 2013, the manager of the broker certification team told us that he was unaware of the executive director's statement to legislators and that MNsure was still requiring brokers to provide their Social Security numbers. In response to our request for clarification, MNsure's general counsel told us the following:

> Upon MNsure first discovering the incident on 9/12, it was still believed that collection of the SSNs [Social Security numbers] was necessary/appropriate. As such, the only adjustment to our collection mechanism was to encrypt the e-mails being sent to brokers for these requests—this was instituted on 9/18. As we gathered more information on this issue, it became clear that collection of the SSNs, while not prohibited, was not strictly necessary to carry out this MNsure business function. Once MNsure gained knowledge that the SSNs were not necessary—on 9/19—a decision was made to stop collecting SSNs from brokers. Following this decision, there was a belief amongst MNsure leadership that this decision was implemented. We subsequently learned that this decision had not been implemented, and clearly communicated that all collection of SSNs should cease and, after 9/27, SSNs were no longer requested from brokers.[15]

The mistake by a MNsure employee resulted in considerable concern and cost, largely because the disclosure included Social Security numbers connected to other personally identifying data. It is now clear that if MNsure had adequately vetted the decision to collect Social Security numbers, those negative consequences would have been avoided. In the next finding, we point out an additional way those consequences could have been avoided by MNsure using a more secure method to collect data from brokers.

[14] See *Minnesota Statutes* 2013, 13.04, subd. 2, for the required elements in a "Tennessen Warning."

[15] Mike Turpin, MNsure General Counsel, e-mail to Cecile Ferkul, Deputy Legislative Auditor for the Financial Audit Division, October 15, 2013.

Finding 4

MNsure decided to collect personal data, including Social Security numbers, from insurance brokers using e-mail without fully assessing and mitigating the risks involved and without considering a more secure and efficient alternative.

As a state agency, MNsure uses an e-mail system that automatically encrypts e-mails while in transit from one state agency to another. However, an e-mail sent to a person outside state government is not secure unless the sender manually triggers encryption. The training MNsure required its employees to complete included information about how to encrypt e-mails and attachments. However, in using the state e-mail system to obtain private data from brokers, MNsure did not use the encryption option. When we asked the manager of MNsure's broker team whether team members received additional training and direction on using the encryption option, he said, "Not until after the incident."

We also asked the manager of MNsure's broker team if MNsure had considered using a software application and a secure Web site to gather data from brokers. This is a common approach organizations use to gather data, including private data from individuals. This approach would not only have provided more security, it also would have been more efficient and eliminated the risk of error when MNsure cut and pasted information from an individual form onto the MNsure Broker Roster. When we asked the manager whether this option was considered, he said:

> So as we moved through the process, this is, you know, decisions we were making fairly quickly, knowing we wanted to get this done and make sure we got through the certification process. There's a lot of interest in becoming certified ahead of October. So we moved along on the e-mail path. You know, I thought once I had vetted it as I did that we were okay. I have never been, previous to this, involved in collecting this type of information from outside entities…. And so [I] thought e-mail would be fine.

In this finding, we again have discussed a decision made by MNsure officials that contributed to the disclosure of private data. In fact, when we asked the manager of the broker certification process if in retrospect MNsure should have used a data collection tool and a secure Web site rather than e-mail to collect private data from brokers, he said: "Certainly. If we had knowledge of it or perhaps done more assessment of the tools available to us, that would have been a preferred option, it sounds like."

Finding 5

MNsure did not adequately secure private data residing on its internal computer network.

To operate its internal business functions, MNsure established an internal network of interconnected computers. Such a network is referred to as an "intranet" and the computers in the network are referred to as "servers." MNsure employees connect to the servers through their MNsure assigned desktop and laptop computers. It is important to note that this internal computer system is separate from the MNsure insurance exchange that individuals use to shop for and obtain insurance.

When MNsure announced that the employee responsible for the disclosure of private data no longer worked for MNsure, the agency indicated that the employee violated a MNsure privacy policy when the Broker Data Roster was copied by the employee onto their local computer. By implication, this suggested that the roster, containing private data, was more secure residing on a server in MNsure's intranet than on the employee's local computer.

According to the information we obtained, the MNsure Broker Data Roster was no more secure on a MNsure server than it was on the employee's local computer since in neither place was the roster encrypted. In addition, we learned that on the server, the roster was accessible to all MNsure staff (approximately 70 people) whether their job duties required access or not.

Finally, we learned that in developing MNsure's internal computer network, the primary objective was to support the organization's business function prior to the opening of MNsure's external insurance exchange. Once the exchange was open and operational, staff planned to go back and tighten security over the internal computer system. That process was accelerated by the unauthorized disclosure of private data on September 12.

Finding 6

MNsure assigned few staff to develop the broker certification process.

In May 2013, MNsure sent an e-mail to insurance brokers licensed in Minnesota requesting that brokers e-mail the agency a "notice of intent" if they wanted to be trained and certified to use MNsure to sell insurance products. In describing the response, the manager of MNsure's broker training and certification process told us the following:

> So we started receiving those e-mails of notices of intent throughout the summer. At that point I didn't have any staff on board to be doing this work. So the e-mails were coming in…. I was working with the navigator team to sort of triage these coming in, and we were —we were holding onto them in a folder until we could get folks started documenting the notices…. At some point

> in June, as we had, I think, getting up close to a thousand e-mails notices of intent from brokers, we did grant access to that account to a couple administrative assistants at MNsure and had them begin the process of logging.

As MNsure was receiving this significant response from brokers, it was also trying to establish the training brokers would be required to complete. In discussing with us that aspect of his responsibilities, the manager of MNsure's broker training and certification process told us the following:

> So what we worked on most of the summer [of 2013] was figuring out how we were going to do the training. We went through a process of analyzing options; were we going to work with third-party vendors that could provide this training that are CE [continuing education] providers certified by Commerce, would we do it ourselves. I was told that we needed to do both and that we needed to be able to offer it for free to brokers as well as work with third-party CE providers and that the training needed to be the same. So we went through that process of determining how that could work. We were on the paths to work with various CE providers, and we were producing our own training.
>
> As the summer went on, you know, we were still not getting all the information we needed to complete the training, and we ran out of time, really, to work with the [continuing education] providers. So at a certain point, we decided we'll wait to work with them until later this fall, and we will just go ahead and provide the certification training ourselves.

Although the staffing level for MNsure's development of a broker training and certification process has varied, it has always been relatively small. For example, according to the manager of MNsure's broker training and certification process, on October 23, 2013, he had one broker coordinator, two administrative staff, and three consultants assigned to his team.

Given the complexity and importance of the responsibility—and the fact that MNsure was legally mandated to establish a broker certification process—we find it questionable that MNsure assigned so few staff to tasks involved.[16] The result appears to be a stressed work environment in which key goals were not achieved in time for MNsure's opening date on October 1, 2013.[17]

---

[16] For the legal mandate, see *Minnesota Statutes* 2013, 62V.05, subd. 3.

[17] In responding to a draft of this finding, MNsure told us that the staffing level reflected the fact that providing continuing education credits for brokers is not required under federal law, and the state requirement did not emerge until late in the 2013 legislative process. As a result, MNsure had not requested staffing for the state requirement in its federal grant, and making staffing adjustments to address this unanticipated responsibility was difficult.

Finding 7

MNsure did not effectively organize the information it collected from brokers.

As noted in a previous finding, on August 13, 2013, the MNsure employee who mistakenly disclosed private data was hired by MNsure and assigned to the broker training and certification team. The employee told us the following:

> And shortly after I started it was determined that we needed to break up different responsibilities and mine was going to be the monitoring of this general e-mail box that comes to MNsure. And it has a myriad of different e-mails that come through it. It is the consumer assisters and navigators, the broker information, and so it's a very heavy usage e-mail that tons of e-mails come through every day. And so it's a triage of getting it to the right person. Answering the broker questions were particularly my area of concern and what I needed to work on. So it was a variety of things that came through, notices of intent, broker certification forms, broker rosters, questions on how MNsure is going to work….

As also noted in the previous finding, on September 12, 2013, the employee sent an e-mail to a broker and mistakenly attached the MNsure Broker Data Roster rather than a spreadsheet for the broker to complete. In an interview, we learned that the employee was unaware that MNsure had already sent the broker a spreadsheet and that he had told MNsure that he was not able to complete it. In an e-mail dated August 20, 2013, the broker told MNsure the following:

> To whom it may concern:
>
> When I attempted to complete the Excel spreadsheet roster form there was not enough room for the e-mail addresses as when entered it spilled in to the next file. What can I do to get around this obvious error? Thanks

In an e-mail dated August 28, 2013, MNsure had told the broker to send the required information to the agency in the text of an e-mail, and approximately two hours later he did, including his Social Security number. When the broker received an e-mail from MNsure on September 12, 2013, saying that MNsure did not have the information it required from him, the broker replied that he had already provided MNsure with the information and that he was willing to send the August 28 e-mail to MNsure again. However, the broker also added the following: "I am beginning to wonder who is minding the store at MNsure."

The MNsure employee's lack of awareness of earlier communications between MNsure and the broker resulted from an inadequate filing and information tracking system. The system did not allow the employee to readily retrieve

MNsure's previous communications with the broker. That deficiency not only created a frustrated broker, it also led to the inadvertent disclosure of private data.

Finding 8

MNsure relied on data security and privacy training that may not have been adequate.

MNsure provided employees with a basic introductory overview of data privacy policies and data protection procedures. However, the general nature of the training, the test questions, the score required to "pass," and the limited ability of supervisors to follow up on areas of concern may not have ensured that employees adequately understood how to protect not public data.

At the time of our review, MNsure required its employees to take two online training courses related to protection of private and other not public data. The employee who mistakenly disclosed private data asserted to us that she had completed both courses, and her supervisor indicated to us that he thought that was true. The two courses have been presented by MNsure officials as being sufficient to ensure that its employees are knowledgeable about their responsibilities to protect private data.

The courses were developed by the Minnesota Department of Human Services for its employees and county social services workers who interact with the public or have access to private and confidential public health data the department collected about individuals who received support or medical benefits through the department. According to the department, the courses were designed to satisfy the training requirements in the federal Health Insurance Portability and Accountability Act (HIPAA), which governs the privacy of an individual's health care records.

The two courses include:

- *Protecting Information Privacy*, which provides an overview of protected data (or, as it is categorized under Minnesota law, "not public" data).[18] It also provides both general and some specific information about how to secure protected data, as well as circumstances when protected data may be shared with others. The knowledge assessment presents the employee with 22 questions (from a set of 60 questions), and the employee must correctly answer at least 70 percent of the questions (16 of 22) to pass the course.

- *Putting Security into Action*, which provides an overview of the habits and behaviors that support both physical and electronic data security at the

[18] Federal laws and the Minnesota Government Data Practices Act use different terminology for data that is not public. Under Minnesota law, data on individuals that is not public is classified as either "private" or "confidential," depending on whether the subject of the data has access to the data. Federal law, and specifically laws related to health records, typically uses the term "protected."

Department of Human Services. It focuses on protecting data by limiting physical access to work spaces and protecting electronic data by controlling access by using strong passwords, virus protection, and following good network practices. The knowledge assessment presents the employee with 12 questions (from a set of 40 questions), and the employee must correctly answer at least 65 percent of the questions (8 of 12) to pass the course.

With a few exceptions, these courses provide only basic information about data privacy laws, the types of data that are protected, and how to ensure protection. The following knowledge assessment questions linked to the courses demonstrate the level of knowledge needed to pass.

- This federal law protects any health-related records that identify an individual, which it defines as Protected Health Information (PHI). (Choices: MN Data Practices Act; MN Health Act; Health Insurance Portability and Accountability Act (HIPAA); or Federal laws relating to substance or chemical treatment.)

- In general, if you administer a state or county program or work directly with clients or others, you are responsible for protecting personal information. (True or False)

- Protected information can exist in electronic, written, or spoken formats. (True or False)

- If I e-mail protected information over the Internet or outside a secured state or county network, the information must be encrypted before I can send it. (True or False)

Supervisors can obtain reports that show whether employees successfully completed the training, but other information is not available. The supervisor cannot, for example, identify employees who had low passing scores or incorrect answers in areas that relate directly to an employee's assigned duties. With this additional information, a supervisor could supplement the training to meet specific employee needs.

Final Comments

MNsure officials have portrayed the unauthorized disclosure of private data as an isolated mistake by an individual employee. In a meeting of the MNsure Legislative Oversight Committee on September 24, 2013, the MNsure board chair said:

> We did our internal investigation [and] we saw no systemic issues.… It's an HR issue; it's been addressed, and we're moving on.

That version of what happened overlooks a series of significant decisions made not by the employee who inadvertently disclosed private data but by others at MNsure. For example, it was others at MNsure, not the employee, who made the decision to collect Social Security numbers from brokers. It was others, not the employee, who allowed Social Security numbers—as well as other personal data—to be transmitted by unsecured e-mail when more secure methods were available. It was others, not the employee, who allocated few staff to the development of a broker training and certification process, making it more likely that mistakes would occur and key tasks would not be accomplished.

The MNsure employee who disclosed private data made a mistake, acknowledged it, and was terminated. However, our findings demonstrate that what occurred was more than "an HR issue" involving one employee. We hope this report will help MNsure more fully and forthrightly understand and acknowledge its part in the unauthorized disclosure of private data that occurred on September 12, 2013.

November 6, 2013

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

Thank you for the opportunity to review and comment on the results of your special review of the inadvertent unauthorized release of private data. Generally, MNsure believes the report is accurate and agrees with its findings. MNsure appreciates and values the thorough examination of this incident and is committed to taking measures to ensure one like it does not occur in the future.

On behalf of MNsure, I would like to once again extend our sincere apologies to the brokers whose information was disclosed. MNsure takes its obligation to protect private data very seriously and are working hard to regain and maintain the public's trust in our organization.

As you have indicated in your report, MNsure took immediate measures to ensure the recipient of the disclosed data deleted the data file and we confirmed that the data file was permanently deleted from the recipient's computer. Since then, MNsure has taken additional actions to address both this incident in particular and to address data privacy and security procedures within MNsure in general. First, in the days immediately following the incident, MNsure conducted work station-by-work station reviews to ensure that our data privacy and security policies are in practice. MNsure has also conducted in-person data privacy and security training sessions with staff to ensure they are familiar with the location of information security policies and have an understanding of computer security practices and to provide in-person guidance on specific privacy and security issues.

Next, in an effort to determine whether modifications to data privacy and security policies may prevent such incidents from occurring in the future, MNsure has engaged the Minnesota Privacy Consultants to perform a root cause analysis of the factors leading to the unauthorized data disclosure. The results of the analysis are expected by mid-December. Finally, MNsure continues

to work with the Minnesota Department of Human Services to update the data privacy and security training that the two organizations will share.

In conclusion, MNsure deeply appreciates the hard work your team put into preparing this report. We will continue to review the issues raised in the report with the goal of strengthening the privacy and security controls MNsure has implemented.

Respectfully,

April Todd-Malmlov
Executive Director