MEETING
MINUTES DRAFT

Board of Directors Meeting

Date: Friday September 20, 2013	**Building:** 81 East 7th Street, St. Paul, MN 55101
Time: 2:00 – 4:30 pm	**Conference Room:** 1st floor atrium
Attendees: Thompson Aderinkomi, Pete Benner (phone), Brian Beutner (phone), Kathryn Duevel, MD, Tom Forsythe, Commissioner Jesson, Phil Norrgard	
Staff: April Todd-Malmlov, Carley Barber	

Topics:

Welcome and any new business *Lucinda Jesson, Temporary Chair*	Commissioner Jesson served as temporary Chair, as Brian Beutner was unable to attend in person. Brian Beutner and Pete Benner attended by phone. No new business.
Approve September 11th meeting minutes *Lucinda Jesson, Temporary Chair*	Phil Norrgard moved to approve the September 11th meeting minutes. Kathryn Duevel seconded and the minutes were approved.
Incident report *April Todd-Malmlov, Executive Director*	April Todd-Malmlov provided the details of the broker roster email incident and the response details. The details are contained in the incident report. April reiterated that the data incident was in no way related to the MNsure IT system, and then took questions from Board members. **Q.** Who is conducting the root cause analysis? **A.** We are in the process of evaluating whether to do that with internal staff or use an external resource. We are looking to DHS for consultation on what has worked well for them in the past. The Board members indicated they would like to use a third party conduct the audit. **Q.** When are we expected to be done with the review? Will it be complete by the next Board meeting? **A.** There are two levels of review. One is the targeted workstation by workstation review. That review is about how are we putting our policies into practice and is occurring today, Monday and Tuesday so information will be available by the September 25th Board meeting. The plan is to also use that time to secure an independent resource to conduct the root cause analysis, which would be a longer term process. The results of that would then be used to inform policies and procedures. **Q.** How are we ensuring we know the staff understands what they've learned in their training? **A.** Staff must pass a competency test. We are also evaluating the training to

determine if there are ways we can make it more practical and conduct it more frequently.

Q. What is the format of the training?
A. It is online training.

Q. Despite the good training, are there measures we are putting into place to prevent similar future breaches?
A. Part of the review will involve reviewing data collected and the purpose for its collection. That will address the administrative control that will prevent this in the future.

Q. While accidental, this is extraordinarily serious. We understand it is a Human Resources issue but is there anything you can tell us?
A. The employee is no longer employed by MNsure.

Q. From a technical perspective, can we remotely survey employee desktops on an ongoing basis to see if they've accessed information?
A. We will explore what controls are available and if we want to implement them.

Q. How are we monitoring the business side of it?
A. There are processes that exist outside the IT system. It's important that we have these policies and that they are followed by all employees. With human use comes human error, but we have policies and procedures in place to reduce these errors.

Q. As we work with third parties, do they adhere to our policies?
A. Yes, they do need to comply and in certain circumstances we need to comply with theirs and our policies must be merged. This is always in the contracts.

Q. Is there a process to know what type of vendor needs to sign this type of contract?
A. We've taken the approach that it's required for all of our vendors.

Q. Are navigators and brokers included in that group?
A. Yes.

Phil Norrgard commented that the email incident was deeply unwelcomed news that must have been unsatisfying to the staffs, who are working so hard to get this in place. Security systems are only as strong as the people using them. We have to keep in mind this is a human resources problem and not a system problem. He appreciates the transparency the staff has shown and thanked them for their earnest honesty and being forthright.

Q. Retrospectively, the list that was accidentally shared should not have existed. What else do we have? How much sensitive information are we handling?
A. There may be paper related to income verification. Some individuals may not file taxes or be located in the databases we are using to verify income. Pay

check stubs, etc. would be checked and verified by staff. We are working with enrollment with public programs. We have worked to reduce the number of manual processes we have. We will have less of that than other states have. There are other states doing most, if not all, of their Medicaid eligibility determinations on paper. People can fill out paper applications. We co-own the systems and processes with DHS and both agencies have responsibility. Those will be protected in the same way they are today, as the same process is being used.

Q. What happens to the data consumers enter into the system?
A. We use the data to determine eligibility and we have data retention requirements under Federal law that are built into the system.

Q. Who has access?
A. Archival data is governed by different access procedures using the "minimum necessary" principal. Definition of security access is a business function working closely with IT security staff.

Q. Kathryn Duevel stressed the need to provide some level of assurance that those who need insurance can still come here and feel comfortable. We know they will be bombarded with negative messages and sound bites, so how are *we* communicating *our* message? What is MNsure going to do to bridge the education gap? What is *our* sound bite to help their level of confidence?
A. We will take that back and revisit it at the next meeting.

Systems security
Carolyn Parnell, Commissioner and Chris Buse, Assistant Commissioner and Chief Information Security Officer, MN.IT

Carolyn Parnell, State CIO and MN.IT Commissioner, and Chris Buse, MN.IT Assistant Commissioner and Chief Information Security Officer provided a detailed presentation on MNsure Systems Security.

Commissioner Parnell said when something like this happens with an employee, it is not uncommon to think there is something wrong with the IT system. She provided an analogy to help clarify. With online banking, she has a level of trust that there are security measures in place to protect her online transactions and that the bank follows the banking industry security rules. In this case, the issue was more like going to a branch office in a bank with an envelope of cash. She has a level of trust they have a process that protects that cash and that the money will be placed into her account. She is hoping to build trust of this system just as people have trust in banking.

The key points from their presentation included:

- MN.IT is responsible for security and infrastructure all the way up to the application. They have been involved from the onset.
- The decision was made early on that the system would be hosted in Minnesota.
- There are many layers of security. Security in the data center, network security, etc.
- Some of best state IT people are assigned to this project. They are the same people in charge of systems that already exist with the same data protection requirements. They are accustomed to that and being

responsible data stewards.

- In 2013 we have access to the latest and greatest technology that we can bake into the system. This is different than patch working new technology to legacy systems.
- We have to meet the standards and certifications of a number of bodies, including our own, which are quite rigorous.
- Security never ends. Security reviews will be done at every change. Whenever there is new code it will be put through a rigorous security analysis.
- We are confident about how we've built security into the system.
- Chris Buse has been very active in this project. He is nationally recognized as a security expert and is very respected for his knowledge. He has experience with large scale IT systems and significant security issues.
- There are not a lot of chances to build a security model from the ground up like we have here. We have a lot of legacy systems in government that we've inherited by default. This was a golden opportunity.
- We conducted an assessment of the compliance needed and the deliverables we needed to meet. A project plan was created.
- We adopted an "all hands on deck staffing philosophy," tapping into the best subject matter experts from across all government to put the system in place.
- We knew the model had to stand up to external validation, which it did. We successfully completed an external security assessment.
- We are building the model at the same time we are building the system.
- The system deals with IRS data, Social Security Administration data, healthcare data (where HIPAA and high tech requirements come into play). The security rules are all federally dictated and very stringent. They were rationalized together into a "security cookbook" called MARS-E (Minimum Acceptable Risk Standards for Exchanges). MARS-E is 1500 pages of detailed information on what needed to be put together.
- A security risk assessment was conducted, from which a 400 – 500 page report was produced that dealt with just IRS.
- We have a dedicated project manager just for the security part of project. Throughout the year we've had at least 6 full time employees working on security at all times, including a security lead, several full time security architects and business analysts. When we got into specific disciplines we brought in subject matter experts, as well.
- In June representatives from the Center for Medicaid and Medicare Services were out and looked at our system to see if we were on track for the October go-live. The IRS was on site for a review in August. We've received IRS approval to operate and connect to the federal hub.
- Independent of that review, we also had an independent security assessor do an assessment against MARS-E. We did this because he knew people would demand it. The assessment is being conducted in three phases. They looked at all documentation to determine if we are in compliance of MARS-E. Knowing issues would come out of that audit, we asked them to return in November to do an independent reassessment and again in January for any final issues.

	The Board members then asked questions. **Q.** What was the selection process for the external validator? **A.** In the state of Minnesota, when we bring in technology vendors we have an open, competitive process. We crafted detailed requirements, published a work order, received bids and then a selection team chose the vendor based on their technical qualifications and cost. **Q.** Who was on the selection team? **A.** Staff from MN.IT and MNsure. **Q.** The state deals with personal information such as names, social security numbers, income information, etc. every day. Is there anything less secure about our system than any other measure of state government where we deal with the same sort of information? **A.** Absolutely not. This system will have the highest security in state government. **Q.** Did you feel the MARS-E requirements had any weak spots? **A.** They were phenomenally stringent. But there were cases where we felt the bar needed to be even higher. For example, with regard to malware. **Q.** What type of data is *not* flowing into MNsure's systems? What do people commonly think is in there that is not? **A.** Things like medical records, claims data and tracking the doctors people see. None of that information is collected or maintained in any exchange/marketplace. **Q.** There are articles saying we will be "bare bones" on day one and referencing that we are in red status on many areas of project. Is any of that related to security? **A.** No, it is not related to the security. **Q.** Are there aspects of the system that are unique to MNsure that we've never seen in another state agency? **A.** The MARS-E framework was helpful and it was unique for it to all be together in one package. Also, we had a relatively short timeframe for the level of sophistication. Though it may be a level of detail that cannot be discussed in a public meeting, the Board requested to be updated on the security evaluations. A "Minnesota Health Insurance Exchange Security Update" handout was provided. It was given to the State Government Finance Committee earlier this year to update them on where we were on security, but it also provides a good overview.
Public comment	**Rich Neumeister** - the scrutiny is not from one party or another. It's from a bipartisan approach from the legislature. There are people who may not like MNsure but all Minnesotans are concerned about the privacy/security. He also heard an employee was terminated because of this. It comes down to

the responsibility of the agency, and the fast pace.

Independent business reviews should be public and are public from other entities. Transparency is very important and we have to live that.

He saw a story on the news about a gentleman who was trying to get Medicaid and the computers were down for 3 days. He encouraged MNsure to be proactive, or the public will step in through legislators.

Dave Racer – he operates an information service where he communicates with 4600 insurance agents across the state. When this happened, his inbox lit up. We have a significant trust problem. There was already a trust problem because the agents feel MNsure threatens their livelihood. How will we win back their trust? Those 4600 agents talk to thousands of Minnesotans. He would be happy to write a private letter about things he has observed.

Public programs update
Chuck Johnson, Deputy Commissioner, DHS

Chuck Johnson joined the meeting to share where we are with the public programs that will be part of MNsure. The details can be found in the presentation. Chuck then took questions from Board members.

Q. When people come in October 1, are they enrolling in Medicaid expansion or Medicaid as it exists today?
A. If someone applies through mnsure they are applying for coverage effective 1/1 which would include expansion. There is also a place where they can indicate they need healthcare now and we would enroll them in the system we have in place today.

Q. Will paper applications be converted by the counties to online records?
A. It would be our goal, if we end up taking paper applications, that the county worker would enter them into the system. We are not expecting to be taking a lot of paper applications, though people do have the option to do them and we do have a process in place for getting them into the system. Paper verifications might be another thing a worker could enter in the system.

Q. How do two systems connect? Is there a gap for people who didn't understand what needed to be done?
A. If they don't understand or do it they'll stay on MinnesotaCare. At their renewal, that is when the issue would be forced and we'll get them onto the new system.

Q. True that they will have a refund at that point?
A. Yes. That's another reason we want to convert quickly.

Q. Why haven't all of the counties signed up to be IPAs (in person assisters)?
A. While not entirely sure, Chuck thought perhaps some counties prefer to stay with cases inside their regular purview. And perhaps other counties, smaller ones in particular, know they will end up doing the work anyway but chose to forego the $70.

Q. Are we concerned some counties will not be supportive of this transition and

more work will be put on DHS and MNsure staff?
A. Not concerned about that being a barrier. The counties are good about working with the people who come to them and getting them to the right service.

Q. When we look at the things we will be doing that the counties had been doing, will MNsure be compensated from the counties for work we take on that lightens their load?
A. Counties would say that in the long term this will result in administrative savings for their county financial workers because a lot of people will be going online and we are doing away with some of the work that is cumbersome for them. In the short term, it's a lot of change and we are bringing 200,000 more people onto public programs. We are lessening their work in the long term, but there will be more people on public programs. It will take a couple years to see where the balance is.

Q. Slide 10 refers to online functionality that will not be available until the Spring of 2014. To what programs does that apply and how many people do we expect will be impacted by that?
A. It refers to all public programs (both MA and MinnesotaCare). It's in the range of 750,000 - 800,000 people. They will still get to select a plan and be enrolled based on our existing process. It just won't be fully automated. This is the same level of service we already provide. It's just a delay in getting to a better way of doing things. *(see next question for follow up/clarification)*

Q. Will people be surprised by that and feel it's something MNsure promised and did not deliver?
A. It will be easier for people to enroll than it is today. The slide only applies to being able to say which health plan they want to select. Since we are moving people onto the new system, most people have already made their selection. This only impacts new enrollees for the short period between January 1 and the Spring, not all 800,000 people.

Thompson commented about how exciting this is. We are essentially taking a population the size of St. Paul and saying "your healthcare is taken care of." Life will be easier for people who have a lot of other things to worry about in addition to healthcare.

Any place where we are asking this population to do something. How we communicate with them will be very important, as well as mechanisms to follow up. We are trying to help, but this is complicated. We are dealing with things that are not easily understood. Communications will be paramount to do what we are trying to do.

Communications over the next six months will be critical. It will require us to do more notices than usual and other things beyond notices to get the message to people about what is changing, what they need to do or not do to effect that change.

County workers are our customers in this regard. Conversion process is critical.

	Q. For those who do not have online capabilities, when they come in can we put them to a computer or will the county workers be helping? There are concerns about that transition. And speaking of security, if we are encouraging them to find free online access, it may not be secure. How are we helping? **A.** To start, it will likely be traditional, where the county workers will sit with people and help them and take their applications. Over time we'll see evolution toward having computer access at the counties.
Public comment	None
Wrap up and any new business *Lucinda Jesson, Temporary Chair*	April Todd-Malmlov provided an update on where we are with the rollout. There are articles about MNsure's "red" status. The project has had a red status the entire time due to the complexity, detail, schedule and the tight timeframe in which we need to adapt to new requirements as we receive them. Putting items in red status is just good project management practice. It shows the areas that need attention and need risk mitigation so we can make sure we are remediating. For example, the Contact Center had been in red, but is up and is operating well. We will not be putting provider quality data on site. It is not required functionality but is something we want to do in the future. For now, we are focusing our efforts on other areas. We will have provider directories available through the public site, not the IT system. Tom Forsythe feels we should do more expectation setting and that transparency is our friend. A bulleted, short timeline of what to expect in the next six weeks was requested. April mentioned that the site is being developed to do that. It explicitly explains when new things are coming. Commissioner Jesson reminded that although people can start signing up in October, the insurance doesn't start until January. Thompson Aderinkomi feels that, as part of our media strategy, we should encourage Minnesotans to not call on 10/1 so we can manage expectations and volume.
4:30 pm Adjourn	Tom Forsythe moved to adjourn the meeting. Thompson Aderinkomi seconded and the meeting adjourned at 4:40 p.m.