

Untitled

5 about 10 states to be working on some of the lessons
6 learned from that earlier experience.

7 I know the National Governors Association
8 is a very powerful organization and I found that my
9 colleague, Professor Pritts, her university was moved
10 by the National Governors Association from Georgetown
11 to Texas, according to her.

12 (Laughter.)

13 SENATOR MOORE: I don't know that Baylor,
14 the University of Texas know yet that you're down
15 there taking away all the Texans for Georgetown.

16 MS. PRITTS: As long as I get the check,
17 I'll be happy.

18 SENATOR MOORE: I'm sure they'll share.

19 I'm going to turn it over to Joy Pritts to
20 introduce the speakers.

21 MS. PRITTS: Good afternoon. I have the
22 pleasure today of introducing our afternoon speakers.

183

1 They included Dr. James Golden with the Minnesota
2 Department of Health and Ms. Victoria Prescott with
3 the Reganstrref Institute. Dr. Golden is Director of
4 the Minnesota Department of Health, Division of
5 Health Policy. He also serves as the project
6 director of the Minnesota Privacy and Security
7 Project, which, as many of you know, is a large
8 multi-state project. Prior to joining the Department
9 of Health, Dr. Golden was the chief operating officer
10 for the Midwest Center for HIPAA Education.

Untitled

11 Ms. Prescott is general counsel and head
12 of business development for the Reganstrref
13 Institute, a medical research institute that has
14 pioneered work of medical informatics, cost
15 information exchange and health care data
16 standardization. She's involved with the Indiana
17 Health Exchange and the Indiana Patient Care Network.
18 She's also working on the Indiana Privacy and
19 Security Project. So we have lots of members before
20 us today who are very familiar with doing a lot of
21 work on these issues at the state level.
22 I'll now turn it over to Dr. Golden to

184

1 begin his presentation.

2 DR. GOLDEN: Thank you, Professor Pritts.
3 I'd like to thank the Alliance for the opportunity to
4 come before you and share some of Minnesota's
5 experiences regarding privacy and security.

6 (Slide.)

7 DR. GOLDEN: Perhaps to set a little bit
8 of a context for the privacy and security project, in
9 2005, the governor and the state legislature made e-
10 Health a priority for the state by establishing the
11 Minnesota e-Health Advisory Committee, which is a
12 26-member body of both public and private sector
13 individuals that represent consumers, payers,
14 providers, public health as well as employers. They
15 were charged the responsibility of advising the
16 commissioner of health on health information

Untitled

17 technology issues and goals.
18 One of those responsibilities that was
19 assigned to the Advisory Committee was to examine
20 critical issues surrounding the security and
21 confidentiality of health information. So they
22 launched the Minnesota Privacy and Security Project.

185

1 That project was also funded as part of the Office of
2 the National Coordinators, SPC, project.

3 (Slide.)

4 DR. GOLDEN: What I'm going to share with
5 you today represents the input and deliberations of
6 over 25 open and public meetings that were comprised
7 of industry stakeholders as well as consumers and
8 privacy advocates and we had over 56 hours of
9 discussion. The goals for the project were really to
10 take a look at the current loss practices and
11 organizations to try to identify what are the most
12 significant privacy and security concerns that were
13 facing those organizations as they looked at how they
14 might implement the electronic exchange of health
15 information.

16 Once we identified what those most
17 significant issues were, how might we address those
18 to try to eliminate or reduce whatever those barriers
19 might be.

20 (Slide.)

21 DR. GOLDEN: One of the things that I
22 think we know and that we've discovered quite early

1 is that regardless of what model of health
 2 information exchange one is looking at, one of the
 3 most important components for success will really be
 4 consumer or patient acceptance or trust of that
 5 system. Kind of based on our work, we found that
 6 patients have a few interests. They want to be able
 7 to either control or at least know what's happening
 8 with their information. That would include such
 9 things as who's accessing it, what information is
 10 being accessed, when is it being accessed and why is
 11 that person accessing it.

12 Patients also have some concerns about a
 13 new electronic environment. While they appreciate
 14 that there might be some benefits associated with the
 15 information being able to be exchanged with their
 16 providers, every time they pick up the newspaper and
 17 see a breach of security in an information system,
 18 they worry about the security of their data. One of
 19 the strong interest they had were to be alerted when
 20 there was a breach of this information.

21 The other thing that we discovered is that
 22 one of the keys is going to be patient education,

1 both from the aspect of what are the benefits of
 2 being able to exchange information as well as what
 3 are the real risks as opposed to the perceived risks.

Untitled

4 (Slide.)

5 DR. GOLDEN: Throughout the discussions,
6 there were three themes that continually rose to the
7 top as the most significant issues. These were very
8 significant issues from the standpoint of their
9 impact. The first was the issue of patient consent.
10 How should patient consent be implemented in a health
11 information exchange. In Minnesota, this is a
12 particularly significant issue because Minnesota
13 probably has the most stringent and protective
14 patient consent requirements in the country. We
15 require patient consent even for the exchange of
16 information for treatment purposes. That's for all
17 information, not just for sensitive conditions.
18 While this is, perhaps, a little more stringent than
19 some of your other states, many states have a similar
20 type of concern because they have patients consent
21 requirements associated with sensitive information
22 where there might be HIV information, mental health

188

1 information or genetic information.

2 The other reason that this is of
3 particular interest is because patients are very
4 interested in how they control their information.
5 Patient consent is one of the primary mechanisms by
6 which that's accomplished. The second issue that we
7 identified we have called operational difficulties in
8 providing and then limiting and monitoring access.
9 This is a bit of a euphemism, I think, for a set of

Untitled

10 interconnected security problems that focus on who
11 should be able to access the patient's information
12 and how do we assure patients that their information
13 is being appropriately accessed. I'll talk a little
14 bit more about that as we go along.

15 The third issue that was of significant
16 concern was liability concerns. That's a liability
17 for the inappropriate disclosure of information. And
18 while you can't necessarily get rid of liability, it
19 does very much help to focus why the other two issues
20 are so important. That's because today organizations
21 don't have a good way of implementing consent into
22 exchanges and they have a lot of concerns about

189

1 liability. Therefore, when they don't know how to do
2 something well and they have liability concerns, the
3 most simple thing to do to reduce those is simply not
4 to exchange the information. That is why we really
5 focused on the other two issues.

6 (Slide.)

7 DR. GOLDEN: Looking at those issues
8 individually, the biggest issue that we saw with
9 patient consent was differences between providers in
10 trying to determine when and how patient consent is
11 required. There might be some differences as well
12 with regard to when and how patient consent should be
13 required from their points of view. What we
14 discovered is what's causing this difference in when
15 and how patient consent should be required we saw a

16 couple of issues.

17 One, we needed to clarify the application
18 of current patient consent requirements to new
19 concepts related to the electronic exchange of
20 information. Many of the consent requirements that
21 we have today are based on paper records or the
22 exchange of paper records that don't anticipate real

190

1 time exchange of information. How do we make the
2 consent requirements consistent with this new type of
3 environment? Again, we also need to focus those
4 requirements on the electronic exchange of
5 information specifically. There's a lot of concern
6 about how do make sure that patient education gets
7 incorporated into the consent. The consent and the
8 time when we elicit that consent from the patient is
9 a wonderful opportunity to provide patients the
10 opportunity to learn more about what the goals and
11 expectations of the exchange of information is and do
12 we incorporate that into the consent requirements.

13 Finally, there's a need for a little bit
14 greater consistency of frameworks across states. For
15 example, in Minnesota, we require a consent for the
16 exchange of all patient information. Yet, our
17 neighboring state, Wisconsin, they have requirements
18 associated with the exchange of mental health
19 records. Even though we both require consent, we
20 wouldn't satisfy each other's consent requirements as
21 an example.

22 (Slide.)

191

1 DR. GOLDEN: The second issue was more of
2 a security issue. This was the difficulties of
3 trying to provide access and then make sure that the
4 access that's being provided is appropriate. In
5 Minnesota, we've taken to calling this the four A
6 problem. What this is, is we need to find a way to
7 authorized people who should be allowed access to
8 patient records. Once you've authorized those
9 people, you need to find some method for
10 authenticating them to see if there really is a place
11 to be when they're trying to access those records.

12 You also need to be sure that you set some
13 access controls within the records so there would be
14 information that's being accessed is appropriate both
15 for the patient and for the type of treatment that's
16 being provided. One of the difficulties associated
17 with this is information systems today really aren't
18 sophisticated enough to put those in as hard controls
19 where the information system takes care of it. You
20 really need to have some behavioral controls or
21 organizational policies associated with limiting the
22 access to the appropriate access.

192

1 Once you have behavioral controls,

Untitled

2 organizational policies, there is some need to make
3 sure those organizational policies and behavioral
4 controls are being followed. Hence, you need
5 auditing. You need some way to audit what
6 information is accessed and what is appropriate for
7 the situation that the provider is faced with.

8 So those are the four A's that we have.
9 For the most part, it's a difficult task because it
10 requires coordination across organizations in ways
11 that traditionally haven't been done. For example,
12 in auditing, I might have the information about
13 whether or not the patient was in, what providers
14 were seeing them and what we were seeing them for in
15 my institution. But over at the place where the
16 information is being accessed, they're going to have
17 the record of what information was accessed and what
18 was pulled across the system.

19 (Slide.)

20 DR. GOLDEN: As we looked at ways to
21 address those four A's, we also looked at a number of
22 difficulties that made solving those problems quite

193

1 difficult. First, you apply security to specific
2 network designs and architectures. In general, most
3 organizations, states don't have that defined at that
4 level. So without a specific architecture, your
5 solutions have to be at a slightly more general
6 level.

7 Additionally, there's quite a lot of work

Untitled

8 going on at the national level, particularly around
9 standards. But we're waiting to see what happens.
10 States are very concerned about getting out in front
11 of some of those and having to repeat the work.
12 Additionally, any solution should preferably be
13 technology neutral and be able to evolve as the
14 technology evolves as well.

15 Finally, many health care organizations
16 really have quite limited experience at this point in
17 exchanging information electronically. Until they
18 get more experience, they're going to continue to be
19 concerned about these issues and move ahead at a very
20 cautious type of pace.

21 (Slide.)

22 DR. GOLDEN: The solutions to these

194

1 issues, from our standpoint, are probably a mix of
2 legal, technological and organizational issues. Some
3 of them, such as the private and patient consent
4 issues, tend to be statutory issues, regulations that
5 are done at most of the states. One of the things
6 that might be helpful there would be some model
7 legislation for the states that might be tiered in
8 ways that states that currently have more restrictive
9 or protective requirements could be at one level.
10 Other states that maybe have a different community
11 standard could be at a different level, but there
12 would still be consistency regardless of which level
13 was chosen. Some of them are more clearly technology

Untitled

14 issues that will continue to evolve as technology
15 improves and there is more experience in this other
16 organizational levels that need to be implemented
17 within all of the various organizations, both public
18 and private. Any solution really needs to provide
19 some flexibility so that, as we gain experience, we
20 have the ability to adapt in ways that really serve
21 the patients to improve the care and to improve
22 patient safety.

195

1 Finally, one of the things that I think
2 solutions need to do is really maintain or enhance
3 the privacy that's afforded to patients. In our work
4 with consumers and privacy advocates, the one thing
5 that they most like about the idea of electronic
6 exchange is really the ability to improve this and to
7 use technology to look at how can you increase the
8 privacy, the security or just understanding what's
9 going on with your information. Thank you.

10 MS. PRITTS: Thank you, Dr. Golden.

11 Ms. Prescott:

12 MS. PRESCOTT: Good afternoon. Thank you
13 for the opportunity to share a little bit about what
14 we do in Indiana. Go Colts.

15 (Laughter.)

16 MS. PRESCOTT: I just want to give you an
17 overview of what I'm going to cover.

18 (Slide.)

19 MS. PRESCOTT: The legal landscape in

20 Indiana, which is quite different from Minnesota,
21 current health information exchange or HIE activities
22 that we do in Indiana, our approach to privacy and

196

1 security and a quick summary of it -- my opinion, at
2 least, of key issues facing the states today and some
3 recommendations for states and possibly some agenda
4 for the State Alliance for e-Health.

5 (Slide.)

6 MS. PRESCOTT: First, the Indiana legal
7 landscape. Our state laws are very favorable to
8 health information exchange uses, all of them --
9 treatment, research, public health and health care
10 operations, which also encompasses quality measures.
11 I just did a quick draft that depicts the spectrum of
12 state law restrictions on use of patient data.
13 HIPAA, as you see on the left, is in green. It's
14 basically the floor. It sets the floor for the
15 restrictions and basically allows the states to
16 impose their own additional restrictions if they want
17 to.

18 Indiana is sort of near the HIPAA floor.
19 We don't impose any consent requirements on the
20 participants in HIE in Indiana, whereas, Minnesota,
21 as you heard, not only has consent requirements even
22 for treatment, it actually expires within a year,

197

Untitled

1 from what I understand. I believe the other states
2 are somewhere in between.

3 (Slide.)

4 MS. PRESCOTT: Current HIE activities,
5 just to give you a short summary in Indiana, this is
6 mostly central Indiana, which is what I'm
7 representing. We have results delivery or what other
8 people call clinical messaging, which is basically
9 the delivery of lab results and other types of
10 results directly to the clinician. I'm going to show
11 you a little bit of that later on. We also have some
12 general sharing of patient clinical data at the time
13 and point of care. So if you come into the emergency
14 department in Indianapolis, you'll be able to extract
15 and pull all the data we have on you and submit it to
16 the doctor. We also deliver medication history to
17 the hospital when the patient admitted or registered
18 at the hospital because they're under our requirement
19 for state accreditation to do a medication
20 reconciliation process. So our medications assist
21 with that.

22 We also have an e-Prescribing application

198

1 that evolved a few months ago. We have physician
2 support such as clinical reminders to providers. We
3 have a quality reporting, which I believe an article
4 was distributed to you, that kind of gives a good
5 summary of an overview of that project. It's just
6 getting underway. It's been underway for year, but

Untitled

7 it's just getting ready to go live with data in the
8 next couple of months. The premise for that is the
9 payers and the providers have come together to
10 approve a set of quality measures, quality metrics,
11 HIV, since we have clinical data and the payers have
12 given us their claims data. We combine the clinical
13 data and the claims data to be able to show what
14 those performance measures are. By tradition, how do
15 you stack up compared to your peers and where do you
16 need to improve? And then the payers pay for that
17 service. They also pay the physicians who want to
18 improve. So it's the basis of the pay-for-
19 performance or pay-for-value.

20 We are also heavily involved in research.
21 Since we are a medical research institute and we're
22 very involved with public health. We assist them on

199

1 behalf of the hospitals who will submit reportable
2 diseases to the State Department of Health on their
3 behalf. We are also a conduit for linking all the
4 emergency departments in the state. There are 69
5 hospitals now out of like 114 to take some
6 registration, some demographic data and submit that
7 to the State Department of Health. We're up to 6000
8 submeds per day to the State Department of Health.

9 We've actually detected some things. In
10 December, there was an outbreak and the system was
11 able to assist and target where that came from.

12 (Slide.)

Untitled

13 MS. PRESCOTT: The approach we have in
14 Indiana basically didn't happen overnight. We
15 started doing this in the early 1990s. There was
16 trust building over time. We started small just with
17 a couple of hospitals sharing a lab. We focused on
18 what's the most valuable information to give to the
19 providers for care, basically, laboratory tests and
20 medications. We also reached, as a community, what
21 uses are appropriate and how to keep in mind patient
22 privacy as things expand and coming up with other

200

1 ways to improve care.

2 We also considered multiple uses of the
3 data. We know people have secondary uses for the
4 data from Day One. Research was on the table from
5 Day One and public health was very important as well.

6 (Slide.)

7 MS. PRESCOTT: It's hard to explain
8 everything in 15 minutes. Basically, we kind of see
9 as the graphic here the data is coming in from the
10 various sources into the HIE. The term "dictionary"
11 in the middle is very important. That's probably
12 where we spent most of our money in mapping the
13 terms, mapping the lab tests because everybody calls
14 it something different. Some places may call a lab a
15 CBC, Complete Blood Count. Some other place they may
16 call it something else, so we have to map a standard
17 set of terms, a standard vocabulary before we can
18 really do anything useful with the data at all. We

Untitled

19 do that. We store it in a repository. We also need
20 to know who the patient is. There's a master patient
21 index to try to do the matching. We also have a
22 global provider index which says who's the doctor

201

1 because that's a lot more complicated than you might
2 as well. Then we have network applications that fit
3 on top of that.

4 On the right-hand side is how you gain
5 access to the data. That is, how do you decide who's
6 going to have access to the data. I won't go through
7 all the different stakeholders there and all the
8 different types of ways they could use the data, but
9 the key here it's negotiated access. It has to be
10 agreed upon in the community and that that is an
11 appropriate use of that patient's data.

12 (Slide.)

13 MS. PRESCOTT: Let me go into a little bit
14 about the security. I was asked today to talk about
15 security and how do you make it secure to protect the
16 patient's data. We have different applications that
17 have different approaches to gain access to the data.
18 it's all community driven consensus on use. The
19 first example is a kind of a low tech example.
20 Actually, we take the data when the patient comes
21 into the emergency department. We get a registration
22 message from the hospital electronically, so we know

1 the patient is there. We automatically pull the data
2 together for that patient and send it the clinical
3 abstract to a printer in the emergency department at
4 the IP address of the printer. We send it there.
5 The person puts it on top of the chart and gives it
6 to the doctor.

7 (Slide.)

8 MS. PRESCOTT: Just a quick example of the
9 abstract is, because the data is all mapped, we're
10 able to kind of summarize the data on that page. It
11 saves lives.

12 (Slide.)

13 MS. PRESCOTT: Another example is lab
14 results that are delivered directly into the
15 physician's EMR, if they have one, which in Indiana
16 it's 20 to 25 percent. In mostly the larger
17 practices, we can do that. The doctor would then
18 just access the lab results in their own system.

19 (Slide.)

20 MS. PRESCOTT: Another way is to have the
21 lab results delivered to a physician practice
22 electronic inbox. They would actually log on and

1 have access to just their own labs they have ordered
2 or they were copied on.

3 (Slide.)

4 MS. PRESCOTT: This is just an example out

5 of that inbox.

6 (Slide.)

7 MS. PRESCOTT: I'm sorry about this
8 animation. I didn't expect it would be here. I took
9 it out. I hope it won't annoy you too much. This is
10 the Indiana Network for Patient Care. It's an online
11 access. Not only can I get the printout when I need
12 it, I can actually log on and drill down more and let
13 me see that lab test and let me see that radiology
14 screen, et cetera. But it's locked down three ways.
15 We don't have logs that mandate certain things in
16 Indiana, but we do go way beyond it as far as
17 securing the data in practice.

18 The first way it's locked down is by time.
19 If you were admitted to the hospital, your record
20 will be open. But then it will only be available
21 until three days after you're discharged. If there's
22 no discharge notice, then a maximum of 30 days. In

204

1 addition, the location is locked, too. It's locked
2 down even by IP address. Only certain devices can
3 have access to the records. So if you're admitted to
4 Community Hospital North, those are the only devices
5 that are allowed access to it. In addition, it's
6 locked down by users. We track who the users are at
7 that particular facility and only allow those users
8 access.

9 (Slide.)

10 MS. PRESCOTT: This is just another

Untitled

11 picture of how it works. The patient is registered
12 at the hospital. The device is registered and the
13 doctor is authorized. Okay, we're going to open it
14 for a limited period of time. And then, of course,
15 the reverse history.

16 (Slide.)

17 MS. PRESCOTT: Just to turn our attention
18 a little bit more to step back and just look at the
19 states in general, quickly setting the stage for that
20 and what can states do and what can maybe the State
21 Alliance for e-Health do.

22 (Slide.)

205

1 MS. PRESCOTT: Setting the stage. I think
2 it's really important as policymakers to understand that
3 HIE policies have a tremendous impact on lots of
4 different areas, such as the technology use, the
5 cost, how long it's going to take to implement,
6 adoption, ongoing maintenance, legal liability and
7 really financial sustainability.

8 You really won't be able to realize the
9 expected benefits of this system if it's not adopted.
10 That's probably the most important one there and
11 sustainable. You have to be able to pay for it, too.

12 (Slide.)

13 MS. PRESCOTT: Key issues facing the
14 states today, the environment in the states is a real
15 quagmire of state laws. We don't really know
16 sometimes which state laws are impacting HIE,

Untitled

17 although the project is really helping bring that to
18 the forefront. The laws were not written with HIE in
19 mind and some of the laws are a conflict.

20 HIE is not really viewed as a priority.
21 There are other crises to deal with in the states,
22 but luckily it is being raised as a priority. It's

206

1 also a distrust in general between stakeholders
2 oftentimes. Either they're highly competitive or
3 there's issues between payers and providers and there
4 are silos of interests that really need to be aligned
5 for the sharing of data to occur.

6 The state also has to wear multiple hats.
7 There's also a lack of understanding, I think, of the
8 complexities involved in the health information
9 exchange and what it's going to actually technically
10 do it. And of course, the biggest one would be the
11 funding and financial sustainability of how are we
12 going to pay for this. It's not really well
13 understood.

14 (Slide.)

15 MS. PRESCOTT: What can states do?
16 Identifying, which is hard in and of itself sometimes
17 and then removing the state law barriers that exist
18 and trying to refrain from passing laws that dictate
19 or constrain, but use the carrot approach instead.
20 Health care is really local. I would encourage the
21 states to support local HIE efforts underway in the
22 community, encourage that and set up some kind of

1 communication method so the state government
2 understands what's going on. If you're a small
3 state, you might consider doing it all yourself.

4 Also, to seed with money, typically, local
5 HIE effort you can give them a carrot as far as you
6 want them to go a certain direction, follow a certain
7 road map, maybe do clinical messaging first or
8 something and follow with specific standards you can
9 encourage conformance and target and limiting the
10 scope.

11 (Slide.)

12 MS. PRESCOTT: How can the State Alliance
13 for e-Health help states address these issues? In my
14 opinion, it would be to try to help the states gain
15 an understanding of the issues. I don't think it's
16 really been clearly set out. There's not really a
17 level playing field. We'd like to drive out some of
18 this misinformation and uncertainty. There's a few
19 different ways you can do that and also encourage the
20 states to support and seed local HIE, survey the
21 states to understand what the burning questions are
22 and try to prioritize it and bringing common issues

1 to the feds, ones that can't be resolved at the state
2 level and to clearly position the State Alliance for
3 e-Health vis-a-vis other groups. There are several

Untitled

4 other things going on at the same time. Thanks very
5 much.

6 MS. PRITTS: Thank you, Ms. Prescott.

7 Now it's my role to try to summarize all
8 this information very briefly. I think this has been
9 a very interesting panel because it really shows the
10 kind of range of interest that this alliance is going
11 to have to address. It's a good example of very
12 different states and different stages of development
13 with different underlying community standards,
14 perhaps, different approaches to consent, but they
15 still face a lot of the very same issues they both
16 address.

17 One of the common things they both address
18 were the issue of trust, both within -- the trust of
19 the patient with the system and between the other
20 players on the system. It's important to have
21 trusting relationships there or the systems won't
22 work. They also both emphasize the dual objective of

209

1 removing unnecessary barriers to the exchange of
2 health information exchange while protecting privacy
3 and that's a balancing act that is probably going to
4 be very difficult to obtain.

5 Security was an issue given the session.
6 Not surprisingly, they both addressed it as being
7 very important. Ms. Prescott, very helpfully, gave
8 us some real clear examples of how security can be
9 addressed in these systems as they actually operate.

Untitled

10 Additionally, they both raised liability concerns.
11 That seems to be cross-cutting issue with the states
12 in the project. They both also stated that there is
13 just this need for education and easily accessible
14 information on a number of topics, including
15 available security mechanisms, health information
16 exchange issues, which can be quite complex and
17 different models.

18 Lastly, they both addressed the issue
19 where the state was dealing with this topic and not
20 necessarily kept up with the pace of the technology.
21 That they were written for a paper world and they
22 needed to be addressed to make sure they don't create

210

1 inappropriate barriers to the exchange of health
2 information exchange.

3 We will now open it to questions.

4 SENATOR MOORE: What we've seen here is
5 maybe two extremes. I'm not sure how to characterize
6 it. In one way, an intense amount of limitation and
7 regulation versus one where basically the federal
8 standard and not much else. I'm wondering if there
9 were things -- if it were your decision and nobody
10 was interfering with that, if there were things that
11 you feel are probably needed to protect privacy or
12 whatever the issue of protection might be called upon
13 to enact?

14 Or Jim, in your case, if you could do away
15 with certain limitations to focus on or do you think

16 everything is perfect?

17 MS. PRESCOTT: I guess I feel that the
18 consent requirements and limitations are pretty
19 important. It's very difficult to administer.
20 There's a lot of issues with respect to who does it.
21 How to get that and there could be some delays in the
22 process. Talking to my physician friends, some of

211

1 them have said, if the doctor has to go get consent
2 to get the lab results from someone else, he'll
3 probably just redo the test instead. It's faster and
4 easier. And that's really wasteful. We shouldn't
5 have to do that. A lot of other issues implementing
6 consent -- if you have to implement consent for a
7 specific type of data like HIV, how does that impact
8 the data owner? I'm trying to think practically. Do
9 you just block the HIV lab test results? Is that
10 enough? Or do you also have to go off the CD4 count,
11 which wouldn't be done unless you have HIV? So how
12 far out do you go if you start passing laws
13 restricting things? It's very difficult for the HIE
14 or whoever is trying to implement a system to outline
15 that or make sure they comply with the law.

16 I think the best way to do it is to not
17 have the laws requiring all this, but to have the
18 providers do it at their level. They are advocates
19 for the patients. They care about the patients.
20 They are trying to make sure the patients are
21 comfortable with the way they are protecting it. I

22 just think it's going to be a lot better in the long

212

1 run and a lot easier to maintain if we do that.

2 DR. GOLDEN: I think one thing in response
3 to your question, Senator. I don't think Minnesota's
4 laws are complicated. As a matter of fact, I think
5 one of the things we've learned during the national
6 project is, in some ways, Minnesota actually has one
7 advantage over some other states. For example, there
8 are some states that have as many as 22 separate laws
9 that have consent requirements that have sprung up
10 around specific conditions. Trying to understand how
11 you implement all those various laws can be very
12 difficult for providers.

13 In Minnesota, we have one law. It just
14 covers everything, pretty much any exchange. So it's
15 actually quite simply from that standpoint. It's
16 just difficult to understand how you incorporate it
17 into the electronic exchange. I would say that the
18 one thing -- in our state there's a very strong
19 interest in maintaining consent and privacy and I
20 think the privacy advocates feel that that's a very
21 important component to protecting their information.
22 I would say that the one thing that might be helpful

213

1 is kind of an honest discussion about what are the

Untitled

2 risks associated with types of exchanges.

3 In a lot of conversations, you kind of get
4 the extremes on both sides. You have the people who
5 are describing risks which, perhaps, are very remote
6 and not the real concerns. Then you have there is no
7 real risk compared to the relative benefits of
8 treatment. And I think it's perhaps a little more
9 honest discussion about where are the risks, what are
10 the benefits and how can we really provide patients
11 some level of control or understanding of what's
12 happening with their information is probably the one
13 thing that would be most useful.

14 Representative Conaway?

15 REPRESENTATIVE CONAWAY: I wonder, in
16 Indiana, physicians upload information into your
17 central data base.

18 MS. PRESCOTT: From the physician offices,
19 some of them do -- the larger practices. The ones
20 that don't really have an EMR don't do anything like
21 that.

22 REPRESENTATIVE CONAWAY: When you

214

1 described the rules that you have around consent, I
2 sat there. I was trying my data as a resident
3 working all over the hospital and I'm wondering if
4 you allowed all the IT addresses in the hospital
5 access to that record or not. Sometimes you get
6 calls from your clinic in cases that have not been in
7 the hospital at that time. Can you access patients

Unti tled

8 while you're on your work rounds in the hospital as
9 just a practical means of a resident's day or a
10 physician's day? How do you deal with the duality of
11 physicians, residents and attendants?

12 MS. PRESCOTT: Right now we only allow
13 access on the patients in the hospitals. So we don't
14 allow access right now to the data if they're in the
15 patient's or in the provider's office unless we are
16 hooked up to their registration system. We are with
17 a couple of the practices. If the patient goes in
18 for care and we're tied into their registration
19 business and we know that the patient is there for
20 care, we can get the record for them.

21 REPRESENTATIVE CONAWAY: So I understand,
22 for certain practices a central database repository

215

1 provides access into the primary care or that
2 physician's office and can access those records and
3 make them available remotely when there's a problem.
4 Is that what you described? I want to make sure I
5 understood what you said?

6 MS. PRESCOTT: Say that one more time.

7 REPRESENTATIVE CONAWAY: If I understood
8 what you said, in some of your outpatient offices,
9 you have a registration agreement with them. Does
10 that mean that that patient in the specialist office,
11 can the specialist then, because you have access back
12 and I'm going to assume it's to the primary care
13 physician's office -- can that specialist then go out

14 and get the information from the primary? Or does
15 the primary care person put that information in the
16 database and the specialist draws that down? You may
17 not have that capability yet. I don't know.

18 MS. PRESCOTT: Right. They would get the
19 whole record from IMPD, which is other people putting
20 data in for that patient. It would be like a direct
21 pull from one of the other offices. It would be just
22 they would get whatever is in the database for that

216

1 particular patient.

2 REPRESENTATIVE CONAWAY: People are
3 uploading data into the central database. You go to
4 the primary care. It's all there and then when I go
5 to that specialist office, I get permission somehow
6 and that specialist or other provider can go in and
7 grab that information from the central database and
8 use it for the episode of care. Is that how it is
9 designed to work.

10 MS. PRESCOTT: Yes, there is no consent
11 required in Indiana for treatment. It is just when
12 you go to the doctor's office, as long as they -- as
13 long as we know that the patient is there for
14 treatment, via the registration message that we
15 receive, then that record is opened up for a limited
16 period of time for that physician to act on. All the
17 data we have on the patient.

18 REPRESENTATIVE CONAWAY: Excellent. I
19 just want to ask this in terms, again, operationally.

Untitled

20 Now under HIPAA, a person comes to the office. Does
21 the person sign that HIPAA consent form? And for
22 both of you, is it your view that that form, I guess,

217

1 is not adequate. That there needs to be sort of a
2 menu. I think of a person who goes in for end of
3 life care, there are a whole menu of things that I
4 would choose. Can you put an incubation tube in?
5 Can you give them any feeding? You can just imagine
6 the concern. If mental health doesn't go here, it's
7 an HIV item. I don't want my medicine or my labs or
8 -- you know, depending on what the policy is. Is
9 that what states want to do have this manualized and
10 people can decide in advance this is what I want?

11 And I guess, Minnesota, you have a sunset
12 for whatever reason. It seems to be very
13 complicated.

14 MS. PRESCOTT: In Indiana, at least,
15 there's no consent form, per say. They have privacy
16 policies that are required to be distributed under
17 HIPAA. So the different entities that are involved
18 do have their privacy policy that talks about it, but
19 there is no consent required in Indiana to be able to
20 use the data to share it for treatment, payment,
21 operations -- whatever HIPAA says basically, you
22 know.

218

Untitled

1 GOVERNOR BREDESEN: We have come to the
2 end of our time for this session. Is there something
3 you wanted to conclude?

4 MS. PRITTS: We did have two other
5 questions that I'd really like to get to.

6 Mr. Rodgers?

7 MR. RODGERS: My question had to do with
8 consent for using the data for secondary. There is
9 no consent. I assume that means even at the
10 physician level the individual is not consenting
11 during treatment to the sharing of information in
12 terms of secondary consent for use of the data in
13 research. Is there consent for that or is it also
14 under the general consent?

15 MS. PRESCOTT: It's good to clarify
16 research. There's two or more actually different
17 types. One is ID, identified, where you take all
18 identifiers, HIPAA identifiers out of the data so you
19 cannot reidentify the patient and we just basically
20 follow HIPAA for that. You don't need consent for
21 the identifiers data. As far as identified, there's
22 a whole structure for that. There's an institutional

219

1 review board at the university we have to go through,
2 even for the identified things because get something
3 like that from the IRB and then, of course, there's a
4 consent required for identified.

5 MS. PRITTS: I'd like to turn to Governor
6 Geringer.

Untitled

7 GOVERNOR GERINGER: Governor Bredesen, if
8 my question would lead to the next part of the agenda
9 of setting priorities, but I wanted to ask a question
10 in the context of one thing that's been discussed
11 several times around the table is can we take an
12 incremental versus a full-blown record approach and
13 how do we do that. It seems there's some merit in
14 starting this whole process of building trust and
15 building confidence as we've seen in the contrast of
16 the two states. I don't know that there's going to
17 be that much of a difference between the two states.
18 It's just the level of patient comfort with what's
19 being done. So the incremental approach might be
20 something that we could discuss. How did Indiana
21 decide to go down that path with very few
22 restrictions where Minnesota is very conservative in

220

1 its incremental approach. Either one of you if you'd
2 like to respond.

3 MS. PRESCOTT: I don't know when we
4 started this. In 1996 or so there was really even
5 envisioned by the state legislature. I think really
6 had any issues that came to the forefront. It wasn't
7 even really thought about and I think it's only been
8 in the last few years that patient consent with a few
9 data breaches that we're aware of and different
10 entities and medical records -- piracy, fraud -- that
11 kind of thing. It's been more at the forefront
12 recently. Indiana did pass a data breach

Untitled

13 notification this past year that's required to notify
14 the patient and anyone you have data on under certain
15 conditions if they have a data breach. It's come
16 more to the forefront recently.

17 DR. GOLDEN: Minnesota has had a long
18 history of data practices issues. We have a
19 Minnesota Government Data Practice Act which controls
20 a lot of the data practices associated with state and
21 government for all units of government data. A lot
22 of that work came out of the work of the Health,

221

1 Education and Welfare in the '70s and some of their
2 work, which was passed generally for state data.
3 Then I think individuals within the state had
4 specific concerns about the sensitivity of their
5 health information. The ability to use that for
6 discrimination purposes and those types of issues.
7 So they just more or less extended a lot of the types
8 of concepts that were applied to governmental data
9 onto health records. So from that standpoint, we had
10 a long history of over 30 years of these types of
11 protections within our state.

12 GOVERNOR GERINGER: Thank you.

13 MS. PRITTS: I think that when you look at
14 the kind of world of state health privacy statutes
15 you'll find that most of them were enacted after the
16 old HEW report came out, but before HIPAA and before
17 a lot of the electronic health information exchange.
18 So a lot of them aren't really designed to address

Untitled

19 some of the issues that we're facing. They do come
20 out from out of a common framework of concerns to be
21 addressed.

22 Since HIPPA some states -- and I'm sure

222

1 you know which ones individually better than I do --
2 there have been some states that have enacted
3 statutes that have actually heightened the protection
4 of health information in certain areas. But overall,
5 when I think of most of the states I've looked at,
6 there's actually been kind of a downward trend in the
7 states trying to make their state laws more like
8 HIPAA, which set a floor, than actually building on
9 top of it.

10 GOVERNOR BREDESEN: Thank you all very
11 much. Thank you both.