2013 SENATE GOVERNMENT AND VETERANS AFFAIRS

SB 2250

2013 SENATE STANDING COMMITTEE MINUTES

Senate Government and Veterans Affairs Committee
Missouri River Room, State Capitol

SB 2250
01/31/2013
Job Number 18069

☐ Conference Committee

Committee Clerk Signature

Explanation or reason for introduction of bill/resolution:

A Bill for an Act relating to privacy of medical records.

Minutes:

Chairman Dever: Opened the hearing on SB 2250.

Senator Sitte, District 35: See Attachment #1 for testimony as sponsor and in support of the bill.

(12:40) Chairman Dever: Noted that it was a lot of information.

Senator Sitte: (Referenced more of the information in her testimony.)

Chairman Dever: In your testimony you referenced different sections, you were referring to subsections not sections of the code, correct?

Senator Sitte: You are correct.

Chairman Dever: Would I be correct if I said that your objection is not the gathering of the information but the integrity of the distribution of the information?

Senator Sitte: That is an excellent way of saying it. I do have a deep objection to the government even meddling in this area of our lives, but what is happening in North Dakota is really good. It is a tribute to our ITD people. We are not having one big pot of information. Each facility will have their own information. It is not going to be kept in one place. We have directed exchange which is better than some states. There are so many people in this room that understand all of this that will be able to explain it better than I. I

have been working with Brad Tridle, an assistant to a Senator Nancy Barto in Arizona who is the prime sponsor on this. Brad is now working for the federal government on patient protection and privacy issues. Sheldon has met him several times. He is working on increasing privacy at a federal level. He has been a wonderful resource.

Chairman Dever: Has this legislation been adopted in Arizona?

Senator Sitte: Yes, something similar. This is the 4th draft that you have because it is suited to North Dakota's needs.

(16:45) Sheldon Wolf, Director, North Dakota Health Information Technology Department: See Attachment # 2 for neutral testimony and proposed amendments. See Attachments #3 and #4 for additional information.

(29:10) Senator Cook: Every North Dakota citizen right now has the opportunity to opt out with the "break the glass option"?

Sheldon Wolf: We do not have the system up and running yet, but they will have that option.

Senator Cook: When?

Sheldon Wolf: To be honest, we had some issues with our vendor that we are trying to work through, but we are getting there. We will have that option before anyone gets information in the system.

Senator Cook: How will knowledge of that option come to me? In a brochure like the one you gave us?

Sheldon Wolf: Yes. And also we just want to give some general information in the TV ads so that people are aware that is happening so when people go in they can have those discussions with their providers. The providers will have the information and the forms. It will also be on our website so they can do it electronically.

Senator Cook: I am probably unique or maybe everyone else is just like me. I get this stuff in the mail and I don't read it. It would be nice if the physician brings this up when I am in there and get it out of the way.

Sheldon Wolf: I agree with you fully. That is the place where we would love to see it go. That is why we are running the TV ads and some newspaper ads in order to make individuals like you and me aware of it so that when you go into the doctor you can have those discussions with them. It will just take some time. It is not an easy thing to do.

Senator Nelson: I know you are testifying neutral, but what I am hearing is that what you are doing now is working and you don't need to change it.

Sheldon Wolf: The plan we have is working really well. I agree with you in that respect. We have done everything that is in the bill. Do we need to put it in to code? I don't know that we do. If you do it really starts making it harder for us to react to federal regulations coming down. It does tie us up to making changes in a timely basis. The federal government is worried about it as well. There was a pilot run where people got into the Dr.'s office they were given an IPad that gave them the information and they were able to say yes or no. I think what will happen in regard to that is if it works really well, within a couple of years, I think we will not have a choice. We will have to be able to react to those types of things. When people are sitting and waiting they can view the information on something like an IPad, but there are also costs associated with that. These things don't happen overnight. Leaving in the opt out/in piece, I think that is a policy decision. I think it is good to have that discussion; whether it is a good thing for North Dakota to be an opt out state or opt in state. As legislators, I do not see that as a bad thing. That is strictly a policy decision. Some of the rest is procedural and it has to be figured out how it will work. That is why we suggested the changes we did.

Vice Chairman Berry: You mentioned where to put this in the interaction with patience; this could very easily be incorporated into the process of rooming a patient.

Sheldon Wolf: I don't disagree with you at all in that respect. Everyone probably has a different intake process and I don't think we want to legislate that. We want to leave it up to the providers.

Vice Chairman Berry: I am not suggesting legislating it. I am just suggesting it. It would be my recommendation for a time to make it easy in implementation.

Sheldon Wolf: It is a great recommendation.

Chairman Dever: You indicate that some provisions in this may be duplicate of federal law; do you see anything in there that is in conflict with federal law?

Sheldon Wolf: There are things in there that are much more restrictive. Some of the reporting requirements are much more restrictive than HIPA. Even if there was something that was in conflict with federal law, the HIPA rules would override state rules anyway unless it is more restrictive.

Chairman Dever:

(37:06) Courtney Koebele, Executive Director, North Dakota Medical Association: Testified to support Sheldon Wolf's recommendations.

(37:55) Dan Ulmer, Blue Cross Blue Shield of North Dakota: Testified in support of Sheldon Wolf's recommendations.

Chairman Dever: Closed hearing on SB 2250.

2013 SENATE STANDING COMMITTEE MINUTES

Senate Government and Veterans Affairs Committee
Missouri River Room, State Capitol

SB 2250
02/01/2013
Job Number 18170

☐ Conference Committee

Committee Clerk Signature

Minutes:

Chairman Dever: Opened SB 2250 for committee discussion. This might require an extensive amendment.

Chairman Dever: My impression of the whole health information network is that the people working with it are really concerned about ensuring the security and the privacy of the information that is contained there. I did not hear them express any real opposition to further protecting and Sheldon did offer amendments on the back of his testimony. I believe that he does not want see us duplicate federal law. It seems that it does not conflict with it. We won't act today but we need to talk about what we want to see changed.

Senator Schaible: (Commented on the concerns of what the federal government could do that would jeopardize what we currently have in North Dakota law and whether or not it requiring the legislature or administrative rule is best.)

(3:28)Senator Cook: On the same line of thought, they seem to want to continue to do things through administrative rules, and maybe that is fine, but the most important thing is that as changes are made, that whether it goes through administrative rules or the legislative process, it creates a process where legislators have to be made aware of changes. It just cannot happen that it all of the sudden effects our citizens. Through legislation the entire legislature has to be made aware of it; unfortunately it takes two years. I always have trouble with the federal government being able to make a decision as freely

as they can through an agency that affects citizens of North Dakota and change North Dakota law.

Chairman Dever: If I received notice of the administrative rule hearing that effected health information, it might be more technical than I am going to want to sit and read through unless I have an awareness or interest in that particular issue.

Senator Cook: Like I said, I don't look at this stuff in the mail.

Vice Chairman Berry: In Sheldon's testimony, it mentioned that they had gotten together with most of the stakeholders and they talked about the opt in/opt out and that by in large they felt that the opt out method was the best, a "break the glass" provision. To Senator Cook's point, I am more comfortable with it being in statute as opposed to it being subject to executive order or administrative rule. It could very easily be put in and you could be asked if you wanted to opt in or out. It allows for letting the patient know face to face what their options are.

Senator Nelson: Having penned in all of the amendments proposed by Sheldon, that is basically what he does. (Goes through how the amendments fit into the bill.)

(Amendments were moved by Senator Nelson, but then they were withdrawn due to the committee wishing to spend more time looking at them and discussing them further.)

Chairman Dever: Closed committee discussion.

2013 SENATE STANDING COMMITTEE MINUTES

Senate Government and Veterans Affairs Committee
Missouri River Room, State Capitol

SB 2250
02/15/2013
Job Number 19021

☐ Conference Committee

Committee Clerk Signature

Minutes:

Chairman Dever: Opened SB 2250 for committee discussion. Reminds the committee what the bill entails and what the amendments were for. There was a meeting between Senator Schaible and Sheldon Wolf and they worked out some amendments.

Sheldon Wolf, Director, North Dakota Health Information Technology Department: See Attachment #1 for hog-house amendment proposed.

(3:25) Senator Schaible: Lisa was also at the meeting and other sponsors were invited. This does what we want it to do without the hindrance of the other language we had. If you are interested in the opt provision, I believe this is the best way to do it. Right now everyone is happy with this.

Chairman Dever: I visited with the prime sponsor too and made the point, and she agreed, that everyone involved with this whole process is concerned about the privacy of individuals and she is just concerned that beyond your control their might be some other concerns. I think those have been addressed.

Sheldon Wolf: I hope so. I am very concerned about privacy. I want to make sure the people's records are maintained and they are not used where they should not be.' That is why we have people hired to do audits behind the scenes. Some of you may be aware that we did terminate our contract with our other vendor that we have for this system, and it was

because of breach of contract issues, not because of breach of records. We are looking to go with another vendor. Trust in your vendor is very important and getting the work done.

Senator Nelson: When you were first here you were neutral on this bill and I have noted here that most of this is already in HIPPA. Have you changed your mind?

Sheldon Wolf: That was related to a lot of the other pieces of the bill that were talking about privacy and security. The opt- out can be either way. That is not in HIPPA rules. They allow opt out or opt in as both a method you can use with it. That is why this piece of it makes sense to me because I think this is a policy decision of the state. If you look at the amendments, this was the piece we had left. We just tweaked it a little bit.

Chairman Dever: Asks committees wishes.

Senator Schaible: Moved the amendments 13.0187.04002.

Vice Chairman Berry: Seconded.

A Roll Call Vote Was Taken: 7 yeas, 0 nays, 0 absent.

Senator Schaible: Moved a Do Pass As Amended.

Senator Cook: Seconded.

A Roll Call Vote Was Taken: 7 yeas, 0 nays, 0 absent.

Senator Schaible: Carrier.

13.0187.04002
Title.05000

Prepared by the Legislative Council staff for
Senator Schaible
February 14, 2013

2/19/13
TD

PROPOSED AMENDMENTS TO SENATE BILL NO. 2250

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact a new section to chapter 23-12 of the North Dakota Century Code, relating to participation in the health information organization.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new section to chapter 23-12 of the North Dakota Century Code is created and enacted as follows:

Voluntary participation in the health information organization - Prohibition on withholding care or benefits.

1. As used in this section:

   a. "Health information organization" means the health information exchange created under chapter 54-59.

   b. "Individually identifiable health information" has the meaning set forth in title 45, Code of Federal Regulations, section 160.103.

2. An individual may opt-out of participating in the health information organization by providing notice to the organization. If an individual chooses to opt-out of participating in the health information organization, the individual's individually identifiable health information may not be accessed by search by a health insurer, government health plan, or health care provider other than the provider who originally created or ordered the creation of the individually identifiable health information.

3. In opting out of participating in the health information organization under this section, the individual must have the option of:

   a. Opting out of participating; or

   b. Conditionally opting out, in which case the accessibility of the individual's individually identifiable health information is limited to access by a health care provider who determines access is required by a medical emergency.

4. An individual's decision to opt-out of participating in the health information organization:

   a. May be changed at any time by the individual by providing written notice to the health information organization.

   b. Does not prohibit use or disclosure of individually identifiable health information which is required by law.

5. A health care provider, health insurer, or government health plan may not withhold coverage or care from an individual nor may a health insurer deny an individual a health insurance benefit plan based solely on that individual's choice to participate or to opt-out of the health information organization."

Renumber accordingly

Date: 2/15

Roll Call Vote #: 1

2013 SENATE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. 2250

Senate Government and Veterans Affairs Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number 13.0187.04002

Action Taken: ☐ Do Pass ☐ Do Not Pass ☐ Amended ☒ Adopt Amendment

☐ Rerefer to Appropriations ☐ Reconsider

Motion Made By Schaible Seconded By Berry

Senators	Yes	No	Senator	Yes	No
Chariman Dick Dever	✓		Senator Carolyn Nelson	✓	
Vice Chairman Spencer Berry	✓		Senator Richard Marcellais	✓	
Senator Dwight Cook	✓				
Senator Donald Schaible	✓				
Senator Nicole Poolman	✓				

Total (Yes) 7 No 0

Absent 0

Floor Assignment

If the vote is on an amendment, briefly indicate intent:

Date: 2/15

Roll Call Vote #: 2

2013 SENATE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. 2250

Senate Government and Veterans Affairs Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number 13.0187.04002

Action Taken: ☒ Do Pass ☐ Do Not Pass ☒ Amended ☐ Adopt Amendment
☐ Rerefer to Appropriations ☐ Reconsider

Motion Made By Senator Schaible Seconded By Senator Cook

Senators	Yes	No	Senator	Yes	No
Chariman Dick Dever	✓		Senator Carolyn Nelson	✓	
Vice Chairman Spencer Berry	✓		Senator Richard Marcellais	✓	
Senator Dwight Cook	✓				
Senator Donald Schaible	✓				
Senator Nicole Poolman	✓				

Total (Yes) 7 No 0

Absent 0

Floor Assignment Senator Schaible

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2250: Government and Veterans Affairs Committee (Sen. Dever, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (7 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2250 was placed on the Sixth order on the calendar.

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact a new section to chapter 23-12 of the North Dakota Century Code, relating to participation in the health information organization.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new section to chapter 23-12 of the North Dakota Century Code is created and enacted as follows:

Voluntary participation in the health information organization - Prohibition on withholding care or benefits.

1. As used in this section:

   a. "Health information organization" means the health information exchange created under chapter 54-59.

   b. "Individually identifiable health information" has the meaning set forth in title 45, Code of Federal Regulations, section 160.103.

2. An individual may opt-out of participating in the health information organization by providing notice to the organization. If an individual chooses to opt-out of participating in the health information organization, the individual's individually identifiable health information may not be accessed by search by a health insurer, government health plan, or health care provider other than the provider who originally created or ordered the creation of the individually identifiable health information.

3. In opting out of participating in the health information organization under this section, the individual must have the option of:

   a. Opting out of participating; or

   b. Conditionally opting out, in which case the accessibility of the individual's individually identifiable health information is limited to access by a health care provider who determines access is required by a medical emergency.

4. An individual's decision to opt-out of participating in the health information organization:

   a. May be changed at any time by the individual by providing written notice to the health information organization.

   b. Does not prohibit use or disclosure of individually identifiable health information which is required by law.

5. A health care provider, health insurer, or government health plan may not withhold coverage or care from an individual nor may a health insurer deny an individual a health insurance benefit plan based solely on that individual's choice to participate or to opt-out of the health information organization."

Renumber accordingly

2013 HOUSE HUMAN SERVICES

SB 2250

2013 HOUSE STANDING COMMITTEE MINUTES

House Human Services Committee
Fort Union Room, State Capitol

SB 2250
March 19, 2013
Job #20138

☐ Conference Committee

Committee Clerk Signature Vicky Crabtree

Explanation or reason for introduction of bill/resolution:

Relating to participation in the health information organization.

Minutes: *See Testimony #1 and 2*

Chairman Weisz opened the hearing on SB 2050.

Sen. Margaret Sitte: From District 35 introduced and sponsored the bill. (See Testimony #1)

10:35
Rep. Laning: How about the case of the person who is comatose? Is there the ability in this that the medical profession can still access the records without their verbal authorization?

Sen. Sitte: Sheldon Wolf can answer that question for you. I think it is provided for. Brad Trydall worked with Sheldon on this. Brad said that instead of saying, "individually identifiable health information", the key phrase to use is, "personal health information".

Rep. Oversen: How does this affect the insurance provider if they are investigating a case to provide coverage?

Sen. Sitte: The exchange of information to the insurance providers will continue. This bill is saying your medical information is not accessible by this state health exchange unless you say so.

14:26
Sheldon Wolf: ND Health Information Technology Director: Provided information on the bill. (See Testimony #2)

18:17
Rep. Laning: How do you go about breaking the glass?

Wolf: There is a popup screen and they say yes this is a medical emergency and gets tracked through the system at that point and time.

Chairman Weisz: If a physician does this, is there a reporting requirement for him after the fact?

Wolf: We will have a report from everyone that breaks the glass and we will take a look at those.

Chairman Weisz: It won't require anything additional on the physician's part?

Wolf: All they need to do is say yes this is a medical emergency.

Chairman Weisz: You would have the ability to come back later and say, what was the medical emergency?

Wolf: Yes. Not everyone will have full access to this, only the physicians.

Rep. Fehr: Accuracy and security question. If you could address accuracy, getting the right person and accuracy of information.

Wolf: If you type in a name, there has to be more than that. You need birthdate and addresses. There is a way the system makes sure you get the right individual. If there were in accurate information, it would happen at a provider level and the person would have to go back to the provider to get that information corrected.

Rep. Fehr: Is it possible that someone can mimic to be a provider?

Wolf: I don't see that happening. The systems are encrypted and they would have to break into the systems through the encryptions and we have a company that is respected worldwide to protect that sort of thing.

Rep. Porter: In regards to other screenings for other insurances. Under this system with my health information on the system, do they have as a registered insurance have access to my information or is there a process they have to go through to get the medical information?

Wolf: There still is a process. You still have to release those records to them. There has to be a process in place for them to do that. They can't just pull up your name.

Rep. Porter: How are you going to handle that influx of business because of that?

Wolf: We won't give them full access and will have to go through a process.

Rep. Porter: What about the patient who wants to look at their record? Can you explain what an appeals process is for an individual to get access to their medical records?

Wolf: Those are addressed under the Health Insurance Affordability and Accountability Act. If you have a request to see your medical information, we will send you back to the individual who has that information. Your clinic has to provide you with your medical information according to HIPPA. If you disagree with something in those records, there is

a process in HIPPA where every provider has to take a look at it and if it wrong, they make the change.

Rep. Porter: I can sign a release and a life insurance company can have electronic access to my information, but I can't do that as an individual?

Wolf: We have a piece in there called the personal health record which would allow some of that information to be available, but not all of it. It is a matter of coordinating all of this down the road. I hope we get to a point and time when you can get all your health information.

Rep. Mooney: In a case where the glass is broken, how long does that take?

Wolf: It is immediate.

Rep. Mooney: The language is under 3b of the bill; "access by a health care provider who determines access if required by medical emergency", is that break the glass clause?

Wolf: Yes.

Rep. Mooney: If a provider should break the glass and deemed it was not a medical emergency, is there a penalty?

Wolf: We will work with provider or organization they are with and they usually have policies and procedures in place in regard to that. Is the person involved going to have to be notified, because it is considered a breech? There are HIPPA rules for that.

Rep. Mooney: What qualifies as a medical emergency?

Wolf: We will work with the providers and organizations to see if it was a medical emergency.

NO OPPOSITION

Chairman Weisz closed the hearing on SB 2250.

2013 HOUSE STANDING COMMITTEE MINUTES

House Human Services Committee
Fort Union Room, State Capitol

SB 2250
March 26, 2013
Job 20466

☐ Conference Committee

Lynnee Thueson

Explanation or reason for introduction of bill/resolution:

Minutes:

Chairman Weisz: This has to do with the Health Information Exchange SB 2250. Anywhere you go, all of your health information will be available to whichever provider you go to. This allows two opt out provisions. One you just say no, the other says only in an emergency. The only new item in the bill is the conditional opt out provision which was already adopted by the HIN committee.

2:09 Representative Mooney: If there is currently an Opt out situation, why would we need additional opt outs?

Chairman Weisz: That wasn't in Code. It was policy adopted by the committee and it didn't have a conditional opt out. This bill does provide the Opt out where if I saw a doctor in Fargo and moved to Bismarck, under this provision, they wouldn't be able to see my information because it wouldn't be an emergency.

3:08 Representative Mooney: So I'm driving down the interstate and I get in a car accident now if I have opted out on an emergency basis and not able to speak then what kind of situation am I leaving myself open to?

Chairman Weisz: Same thing as we are currently. They don't necessarily know what medication I'm on because if there are no family members there or someone they can contact, that's the reason the Feds have pushed this exchange. If it's an emergency go ahead you have access but otherwise I don't want all of the providers visited prior, no access is available.

4:58 Representative Silbernagel: I **move a Do Pass** on SB 2250. Seconded by Representative Hofstad.

A Do Pass Roll Call vote on Engrossed SB 2250: **Yes = 10**, **No = 1**, **Absent = 2**. **Carrier**: Representative Looysen

Date: 3-26-13
Roll Call Vote #: 1

2013 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 2250

House Human Services Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number

Action Taken: ☒ Do Pass ☐ Do Not Pass ☐ Amended ☐ Adopt Amendment

☐ Rerefer to Appropriations ☐ Reconsider

Motion Made By Rep. Silbernagel Seconded By Rep. Hofstad

Representatives	Yes	No	Representatives	Yes	No
CHAIRMAN WEISZ	✓		REP. MOONEY		✓
VICE-CHAIRMAN HOFSTAD	✓		REP. MUSCHA	✓	
REP. ANDERSON	✓		REP. OVERSEN	✓	
REP. DAMSCHEN	✓				
REP. FEHR	A				
REP. KIEFERT	✓				
REP. LANING	✓				
REP. LOOYSEN	✓				
REP. PORTER	A				
REP. SILBERNAGEL	✓				

Total (Yes) 10 No 1

Absent 2

Floor Assignment Rep. Looysen

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2250, as engrossed: Human Services Committee (Rep. Weisz, Chairman) recommends **DO PASS** (10 YEAS, 1 NAYS, 2 ABSENT AND NOT VOTING). Engrossed SB 2250 was placed on the Fourteenth order on the calendar.

2013 TESTIMONY

SB 2250

Attachment #1

Testimony on Senate Bill 2250
Senate Government and Veterans Affairs Committee,
January 31, 2013

Mr. Chairman, and members of the committee, I am Senator Margaret Sitte from District 35 in Bismarck.

Who has access to your personal medical records? Do you even realize the government is now in control of all medical records? Do you know that each person will have an Electronic Health Record by January 1, 2014? These questions are central to the proposed SB 2250, a proposed new section of law to address privacy of medical records.

Please refer to Attachment 1, Inside the Fence

In addition the police have access to all pharmaceutical records.

Next, please refer to Attachment 2, a PowerPoint presentation I attended last year by Dr. Deborah Peel.

Attachment 3 is an Article in the Wall Street Journal by Dr. Peel explaining how patients are shunning health care because of privacy concerns.

Attachment 4 demonstrates just how easy it is for "anonymized" information to be linked to a specific person.

So now that we know the problem, what can states do about it? Arizona passed a health information privacy law, and the bill you see before you is modeled on that legislation. I serve on the Information Technology Committee, and during the interim, I met with representatives of the Information Technology Department, North Dakota Medical, hospitals and others in an effort to make the Arizona bill fit North Dakota's needs. As you can, this bill is our fourth draft, and I think we have had everyone at the table in agreement on this version.

The goal of this health information privacy law is to codify in law what is current policy because policy can change quickly, but this information is too important to be left to chance.

Section 1 sets forth the definitions to be used in this section of law.

Section 2 lists the rights of an individual, including 1) opting out of the health information records system, 2) requesting a copy of one's health information, 3) amending incorrect personal health information, and 4) requesting disclosures of one's information during the past three years.

Section 3 makes it clear that participation in the health information records system is voluntary and opting out will not be cause for withholding care or benefits.

Section 4 requires the health information network to provide citizens with written information describing health information practices, including what information is collected, the categoris of people having access to the information, the purposes for which the information was accessed, the patient's right to opt out, and instruction on how to opt out.

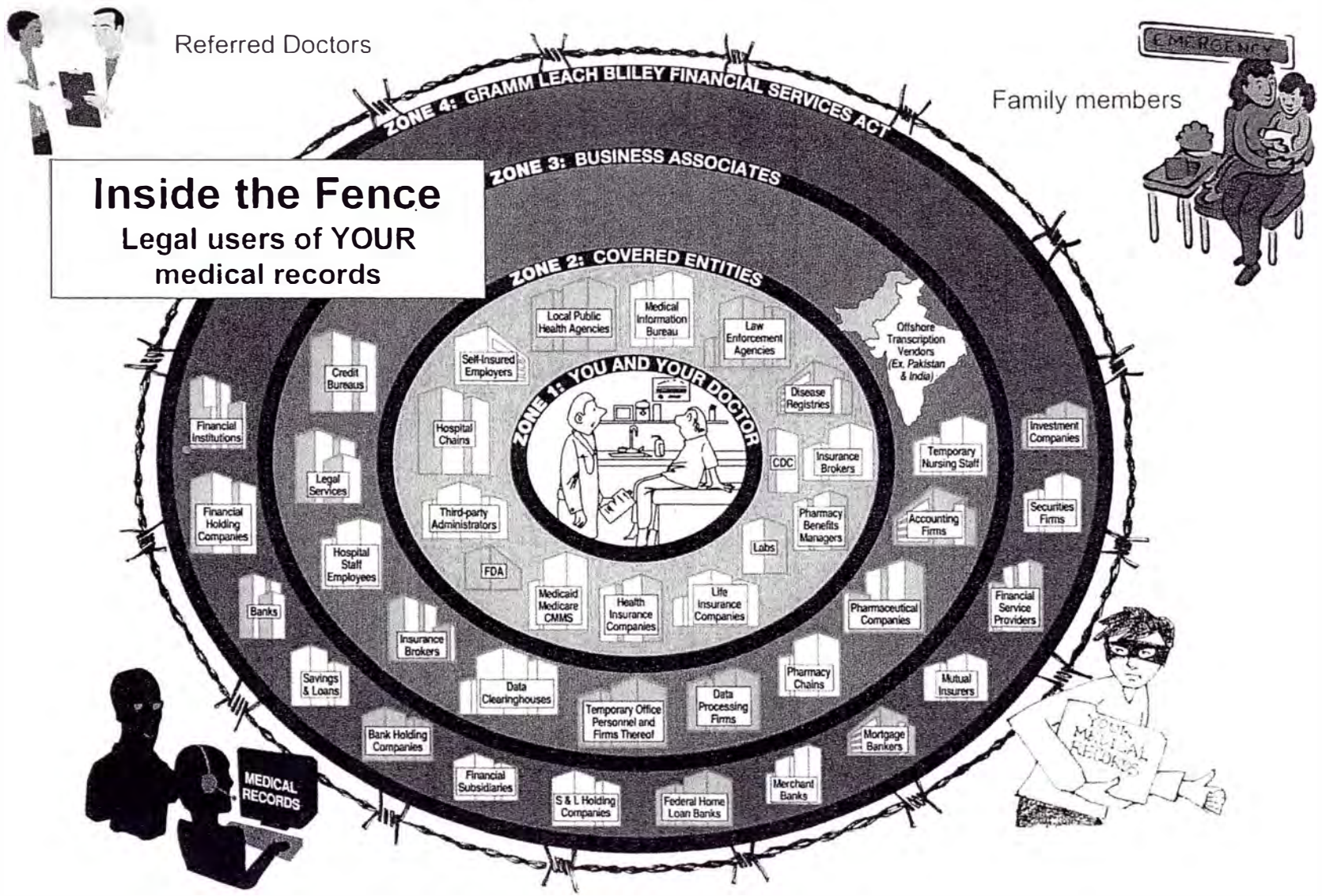
Section 5 lists the responsibilities of the health information network in 1) not disclosing information of those who have opted out, 2) not selling or making commercial use of individually identifiable health information without written consent of the individual, and 3) not disclosing individually identifiable health information for research unless in accordance with this particular section of federal regulations.

Section 6 describes the required policies of the health information network.

Section 7 gives the health information until August 1, 2016 to get the opt-out system up and running.

This bill is all about transparency and accountability. I challenge you to ask five friends if they know that the state and federal government are consolidating their medical records in one central system. I've asked 10, and not one person knew it.

This legislative assembly owes it to the citizens of North Dakota to ensure that they have as much privacy with their doctor as we can possibly secure for them. Hippocrates would remind us that privacy is a foundational principle of quality health care.



www.patientprivacyrights.org

The American Legislative Exchange Council
States & Nation Policy Summit

Arizona Healthcare Reforms: Will States Build Trustworthy Electronic Health Systems?

December 1, 2011

Deborah C. Peel, MD

patientprivacyrights

3 Biggest Myths about HIT

- HIPAA protects privacy
- de-identified data is safe
- we have to give up privacy to benefit from health IT

Reality

- **No data privacy** = individuals can't control personal health data
- **Data isn't secure** = breaches
- $29B in stimulus funds buys model T's
- Health data = $$$$$ commodity
- Risks of HIT outweigh the benefits

More Reality

- 2014: every American will have EHR
- Bush & Obama support building health IT BEFORE fixing privacy & security
- **NO data map** - we have no idea where health data goes
- **Unseen**: Govt & health data mining industry use and sell patient data

What does 'privacy' mean?

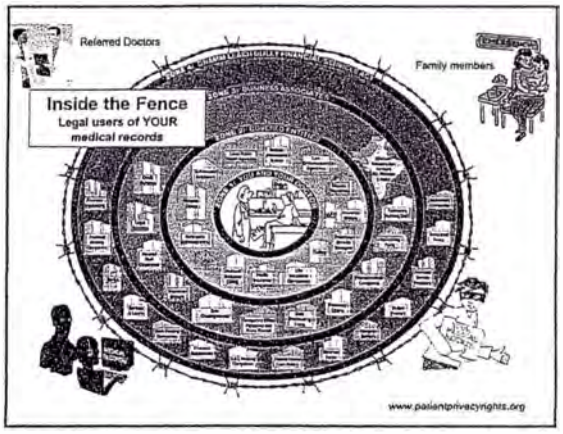
The *NCVHS* defined health information privacy as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data".

(June 2006, NCVHS Report to Sec. Leavitt, definition originally from the IOM)

HHS eliminated the right of consent from HIPAA in 2002

HIPAA regs eliminated consent and privacy

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients' rights to health privacy. Public Law 104-191	*"... the Secretary of Health and Human Services shall submit to [Congress]...detailed recommendations on standards with respect to the privacy of individually identifiable health information."*
2001	President Bush implemented the HIPAA "Privacy Rule" which recognized the "right of consent". HHS wrote these regulations. 65 Fed. Reg. 82,462	*"...a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*
2002	HHS amended the HIPAA "Privacy Rule", eliminating the right of consent. 67 Fed. Reg. 53,183	*"The consent provisions...are replaced with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*



huge market for health data

+

theft and sale of health data

health data mining industry

Where did this slide come from ? The Medical Information Bureau website. The MBI sells claims/health data to insurers and employers.

HIPAA loopholes allow sale of data from EHRs, PHRs, claims data,
lab data, prescriptions, health searches, state data, newborn bloodspots, etc. etc.

Health IT and HIE: 2 separate worlds

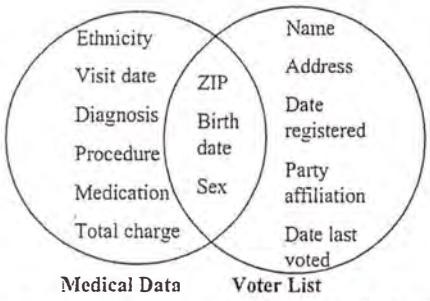
Corporations & Govt

- Industry-centered system
- $29 billion to buy health IT NOW
- Data flows outside US
- Data is a commodity = $$$$
- massive data flows and 2ndary use of sensitive personal data
- No patient consent = DATA THEFT
- Robust HIT systems
  - One hospital = 200+ HIT systems
- Vendors and users sell data
- Massive security flaws
- "Wild West"– data mining and sale for profit and discrimination
- Unfair and deceptive trade practices
- No liability

Patients, Family, & Doctors:

- Not "patient-centered"
- Hardly any data
- No control over health data
- Limited access to personal data
- Limited benefits from HIT
- Massive harms/risks from HIT/HIE
- Limited recourse from harms
- Can't restore data privacy = no way to "make whole" or repair exposure
- Generations of discrimination
- Secret health data bases
- No transparency/accountability
- No privacy and weak security
- Patient Safety—EHRs can harm, be source of errors, can't delete/amend

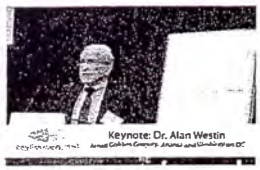
Linking to re-identify data



L. Sweeney. Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine and Ethics*. 1997. 25:98-110.

why privacy matters

people act NOW to protect privacy, numbers will grow



healthprivacysummit

U.S. divides into three groups:

--The Privacy Intense ..... about 35-40%

-- The Privacy Pragmatic ..... about 50-55%

-- The Privacy Unconcerned ..... about 10-15%

http://patientprivacyrights.org/wp-content/uploads/2011/06/AFW-SUMMIT-6-13-11.pdf

refuse diagnosis and treatment

- HHS estimated that **586,000** Americans did not seek earlier cancer treatment due to privacy concerns.
- HHS estimated that **2,000,000** Americans did not seek treatment for mental illness due to privacy concerns.
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.

65 Fed. Reg. at 82,777

refuse diagnosis and treatment

The Rand Corporation found that 150,000 soldiers suffering from PTSD do not seek treatment because of privacy concerns

The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years

"Invisible Wounds of War", the RAND Corp., p. 436, (2008)

act to protect privacy

The California Health Care Foundation found that **1 in 8** Americans have put their health at risk *because of privacy concerns*:

- Avoid seeing their regular doctor
- Ask doctor to alter diagnosis
- Pay for a test out-of-pocket
- Avoid tests

http://patientprivacyrights.org/2005/11/national-consumer-health-privacy-survey-2005/

public expectations

Hippocrates

"Whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will keep inviolably secret."

The ethical codes of all the health professions require informed consent before use or disclosures of personal health information.

"Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients, disclosing information only with the authorization or the patient or when necessary to protect an overriding public interest, such as public health.

Comparable provisions are now contained in the codes of ethics of virtually all health professionals."

Report to HHS, NCVHS (June 22, 2006)

weak security ⇒ breaches, **fraud, data theft & data sales**

Data breaches cost the healthcare Industry an estimated $6.5 Billion

Study Reveals Data Breaches due to sloppy mistakes and unsecured mobile devices --- patients' information is at HIGH risk

Ponemon INSTITUTE

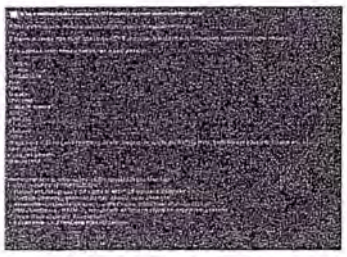
- Data breaches up 32%
- employee negligence key cause
- 73% of providers lack funds to prevent data breaches
- 80% use mobile devices -- but ½ not secure!
- patients discover 35% of breaches
- 29% of breaches cause medical ID theft

Cybercrime—
purchasers want health data

- seeks data to file false medical claims:

Cybercrime—health data for sale

- post seeks buyers for > 6,500 medical records



FEDERAL BUREAU OF INVESTIGATION
NEW YORK

Department of Justice Press Release

For Immediate Release
October 13, 2010

United States Attorney's Office
Southern District of New York

Manhattan U.S. Attorney Charges 44 Members and Associates of an Armenian-American Organized Crime Enterprise with $100 Million Medicare Fraud

Defendants Also Charged with Racketeering, Identity Theft, and Money Laundering Crimes Armenian "Vor" Charged with Protecting Alleged Medicare Fraud Scheme

Is the US the most intrusively surveilled nation among Western democracies?

NHS told to abandon delayed IT project

theguardian

£12.7bn computer scheme to create patient record system is to be scrapped after years of delays

Denis Campbell. Wednesday 21 September 2011

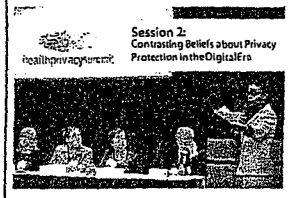
- The NHS has spent billions of pounds on a computerised patient record and booking system, which has never worked properly.
- The £12.7bn National Programme for IT is being ended after years of delays, technical difficulties, contractual disputes and rising costs.

http://www.guardian.co.uk/society/2011/sep/22/nhs-it-project-abandoned?INTCMP=SRCH

realistic solutions

technical:
electronic consent systems
effective de-identification—
no data release without testing to be sure <.04 % can be re-identified
legal: sensible legal and regulatory framework

learn about privacy and security FAST



healthprivacysummit

SEE THE GREAT SESSIONS FROM

1st International Summit on the Future of Health Privacy at:

www.healthprivacysummit.org

Deborah C. Peel, MD
Founder and Chair
(O) 512-732-0033

dpeelmd@patientprivacyrights.org

www.patientprivacyrights.org

patientprivacyrights

The elimination of consent

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients' rights to health privacy. *PL 104-191, Sec 264*	*"... the Secretary of Health and Human Services shall submit to [Congress]...**detailed recommendations on standards with respect to the privacy of individually identifiable health information."***
2001	President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent". *65 Fed. Reg. 82,462*	*"....a covered health care provider **must obtain the individual's consent,** in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*
2002	HHS amended the HIPAA "Privacy Rule", eliminating the "right of consent". *67 Fed. Reg. at 53,211*	*"The **consent provisions...are replaced** with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*

Dr. Peel, a psychiatrist in private practice, is the founder of Patient Privacy Rights (www.patientprivacyrights.org) and leads the bipartisan Coalition for Patient Privacy.

THE WALL STREET JOURNAL.
WSJ.com

OPINION | March 23, 2010

Your Medical Records Aren't Secure

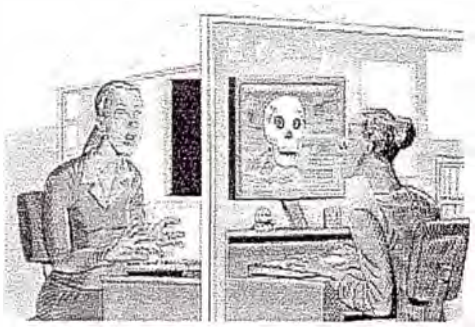
The president says electronic systems will reduce costs and improve quality, but they could undermine good care if people are afraid to confide in their doctors.

By DEBORAH C. PEEL

I learned about the lack of health privacy when I hung out my shingle as a psychiatrist. Patients asked if I could keep their records private if they paid for care themselves. They had lost jobs or reputations because what they said in the doctor's office didn't always stay in the doctor's office. That was 35 years ago, in the age of paper. In today's digital world the problem has only grown worse.

A patient's sensitive information should not be shared without his consent. But this is not the case now, as the country moves toward a system of electronic medical records.

In 2002, under President George W. Bush, the right of a patient to control his most sensitive personal data—from prescriptions to DNA—was eliminated by federal regulators implementing the Health Insurance Portability and Accountability Act. Those privacy notices you sign in doctors' offices do not actually give you any control over your personal data; they merely describe how the data will be used and disclosed.



Martin Kozlowski

In a January 2009 speech, President Barack Obama said that his administration wants every American to have an electronic health record by 2014, and last year's stimulus bill allocated over $36 billion to build electronic record systems. Meanwhile, the Senate health-care bill just approved by the House of Representatives on Sunday requires certain kinds of research and reporting to be done using electronic health records. Electronic records, Mr. Obama said in his 2009 speech, "will cut waste, eliminate red tape and reduce the need to repeat expensive medical tests [and] save lives by reducing the deadly but preventable medical errors that pervade our health-care system."

But electronic medical records won't accomplish any of these goals if patients fear sharing information with doctors because they know it isn't private. When patients realize they can't control who sees their electronic health records, they will be far less likely to tell their doctors about drinking problems, feelings of depression, sexual problems, or exposure to sexually

transmitted diseases. In 2005, a California Healthcare Foundation poll found that one in eight Americans avoided seeing a regular doctor, asked a doctor to alter a diagnosis, paid privately for a test, or avoided tests altogether due to privacy concerns.

Today our lab test results are disclosed to insurance companies before we even know the results. Prescriptions are data-mined by pharmacies, pharmaceutical technology vendors, hospitals and are sold to insurers, drug companies, employers and others willing to pay for the information to use in making decisions about you, your job or your treatments, or for research. Self-insured employers can access employees' entire health records, including medications. And in the past five years, according to the nonprofit Privacy Rights Clearinghouse, more than 45 million electronic health records were either lost, stolen by insiders (hospital or government-agency employees, health IT vendors, etc.), or hacked from outside.

Electronic record systems that don't put patients in control of data or have inadequate security create huge opportunities for the theft, misuse and sale of personal health information. The public is aware of these problems. A 2009 poll conducted for National Public Radio, the Kaiser Family Foundation and the Harvard School of Public Health asked if people were confident their medical records would remain confidential if they were stored electronically and could be shared online. Fifty nine percent responded they were not confident.

The privacy of an electronic health record cannot be restored once the contents are sold or otherwise disclosed. Every person and family is only one expensive diagnosis, one prescription, or one lab test away from generations of discrimination.

The solution is to insist upon technologies that protect a patient's right to consent to share any personal data. A step in this direction is to demand that no federal stimulus dollars be used to develop electronic systems that do not have these technologies.

Some argue that consent and privacy controls are impractical or prohibitively costly. But consent is ubiquitous in health care. Ask any physician if she would operate on a patient without informed consent.

There is no need to choose between the benefits of technology and our rights to health privacy. Technologies already exist that enable each person to choose what information he is willing to share and what must remain private. Consent must be built into electronic systems up front so we can each choose the levels of privacy and sharing we prefer.

My organization, Patient Privacy Rights, is starting a "Do Not Disclose" petition so Americans can inform Congress and the president they want to control who can see and use their medical records. We believe Congress should pass a law to build an online registry where individuals can express their preferences for sharing their health information or keeping it private. Such a registry, plus safety technologies for online records, will mean Americans can trust electronic health systems.

Privacy has been essential to the ethical practice of medicine since the time of Hippocrates in fifth century B.C. The success of health-care reform and electronic record systems requires the same foundation of informed consent patients have always had with paper records systems. But if we squander billions on a health-care system no one trusts, millions will seek treatment outside the system or not at all. The resulting data, filled with errors and omissions, will be worth less than the paper it isn't written on.

"Anonymized" data really isn't—and here's why not
Companies continue to store and sometimes release vast databases of " ...
by Nate Anderson - Sept 8 2009, 6:25am CDT

The Massachusetts Group Insurance Commission had a bright idea back in the mid-1990s—it decided to release "anonymized" data on state employees that showed every single hospital visit. The goal was to help researchers, and the state spent time removing all obvious identifiers such as name, address, and Social Security number. But a graduate student in computer science saw a chance to make a point about the limits of anonymization.

Latanya Sweeney requested a copy of the data and went to work on her "reidentification" quest. It didn't prove difficult. Law professor Paul Ohm describes Sweeney's work:

At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. In a theatrical flourish, Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office.

Boom! But it was only an early mile marker in Sweeney's career; in 2000, she showed that 87 percent of all Americans could be uniquely identified using only three bits of information: ZIP code, birthdate, and sex.

Such work by computer scientists over the last fifteen years has shown a serious flaw in the basic idea behind "personal information": almost all information can be "personal" when combined with enough other relevant bits of data.

That's the claim advanced by Ohm in his lengthy new paper on "the surprising failure of anonymization." As increasing amounts of information on all of us are collected and disseminated online, scrubbing data just isn't enough to keep our individual "databases of ruin" out of the hands of the police, political enemies, nosy neighbors, friends, and spies.

If that doesn't sound scary, just think about your own secrets, large and small—those films you watched, those items you searched for, those pills you took, those forum posts you made. The power of reidentifiation brings them closer to public exposure every day. So, in a world where the PII concept is dying, how *should* we start thinking about data privacy and security?

Don't ruin me

For almost every person on earth, there is at least one fact about them stored in a computer database that an adversary could use to blackmail, discriminate against, harass, or steal the identity of him or her. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm.

Examples of the anonymization failures aren't hard to find.

When AOL researchers released a massive dataset of search queries, they first "anonymized" the data by scrubbing user IDs and IP addresses. When Netflix made a huge database of movie recommendations available for study, it spent time doing the same thing. Despite scrubbing the obviously identifiable information from the data, computer scientists were able to identify individual users in both datasets. (The Netflix team then moved on to Twitter users.)

In AOL's case, the problem was that user IDs were scrubbed but were replaced with a number that uniquely identified each user. This seemed like a good idea at the time, since it allowed researchers using the data to see the complete list of a person's search queries, but it also created problems; those complete lists of search queries were so thorough that individuals could be tracked down simply based on what they had searched for. As Ohm notes, this illustrates a central reality of data collection: "data can either be useful or perfectly anonymous but never both."

The Netflix case illustrates another principle, which is that the data itself might seem anonymous, but when paired with other existing data, reidentification becomes possible. A pair of computer scientists famously proved this point by combing movie recommendations found on the Internet Movie Database with the Netflix data, and they learned that people could quite easily be picked from the Netflix data.

Such results are obviously problematic in a world where Google retains data for years, "anonymizing" it after a certain amount of time but showing reticence to fully delete it. "Reidentification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization," Ohm writes. "This is no small faith, for technologists rely on it to justify sharing data indiscriminately and storing data perpetually, all while promising their users (and the world) that they are protecting privacy. Advances in reidentification expose these promises as too often illusory."

For users, the prospect of some secret leaking to the public grows as databases proliferate. Here is Ohm's nightmare scenario: "For almost every person on earth, there is at least one fact about them stored in a computer database that an adversary could use to blackmail, discriminate against, harass, or steal the identity of him or her. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm. Perhaps it is a fact about past conduct, health, or family shame. For almost every one of us, then, we can assume a hypothetical 'database of ruin,' the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given access to it to our worst enemies."

Because most data privacy laws focus on restricting personally identifiable information (PII), most data privacy laws need to be rethought. And there won't be any magic bullet; the measures that are taken will increase privacy or reduce the utility of data, but there will be no way to guarantee maximal usefulness and maximal privacy at the same time.

There are approaches that can reduce problems. Instead of releasing these huge anonymized databases, for instance, make them interactive, or have them report most results in the aggregate. (But such techniques sharply limit the usefulness of the data.)

Ohm's alternative is an admittedly messier system, one that can't be covered with simple blanket laws against recording Social Security numbers or releasing people's name and addresses. Such an approach has failed, and now looks like playing "Whac-A-Mole" with personal data. "The trouble is that PII is an ever-expanding category, writes Ohm. "Ten years ago, almost nobody would have categorized movie ratings and search queries as PII, and as a result, no law or regulation did either." Expanding privacy rules each time some new reidentification technique emerges would be unworkable.

Instead, regulators will need to exercise more judgment, weighing harm against benefits, and the rules may turn out to be different for crucial systems like healthcare. At the same time, the US needs comprehensive legislation on data privacy to set a minimum threshold for all databases, since Netflix, AOL, and others have made clear that we have no real idea in advance which pieces of seemingly harmless data will turn out to identify us and our secrets.

http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

Attachment # 2

TESTIMONY BEFORE THE SENATE GOVERNMENT AND VETERAN'S AFFIARS COMMITTEE SENATE BILL 2250 JANUARY 31, 2013

Mr. Chairman, members of the committee, I am Sheldon Wolf, the ND Health Information Technology Director. I am here today to provide information on Senate Bill 2250 on behalf of the Health information Technology (HIT) Office and the Health Information Technology Advisory Committee (HITAC).

We agree with the sponsors of this bill that protection of patient information and the choice of participation in the health information network are of the utmost importance to the citizens of North Dakota. Therefore, HITAC, the domain workgroups, legal counsel, and the HIT office have spent a considerable amount of time ensuring that the system we utilize is secure, can be trusted by patients, and allows a patient to have a choice of participation.

To ensure trust, we have developed contracts, policies and procedures, and by statute are currently working on administrative code (54-59-26.2(d)) to ensure privacy and confidentiality. If you are interested in reviewing the policies and procedures we have in place, please visit our website at http: www.ndhin.org/policies. If you wish to see the participation agreements and business associates agreement, they are at: http://www.ndhin.org/services/ndhin-direct/direct-enrollment.

During the interim, we had the opportunity to review this proposed legislation and have provided input into some of the changes to the bill. However, we only provided substantive changes that matched North Dakota's drafting style. We did

not attempt to make major substantive changes to the bill as we understood that the sponsor wanted the bill to follow what Arizona utilized.

However, since this bill has been circulated and submitted, we have received a lot of comments that you should consider. The foremost comment that I have heard is that a lot of the bill is a reiteration of regulations that are currently included in the health insurance portability and accountability act (HIPAA), are already included in the proposed administrative code, regulations and brochures, thus minimizing the need for them to be included in century code.

Additionally, some of the proposed legislation provides an undue burden on providers that they may never be able to meet i.e. to obtain signatures from patients that requires them to determine if a patient has "received, read and understood" the notice of health information practices and whether the patient has chosen to opt out (line 20 page 4).

From what I have been told, the Legislature has tried not to codify federal regulations as providers are already required to follow them and every time they are updated, the century code needs to be update. When this happens, a provider must evaluate and consider which one or both they must implement. This creates a burden on health care providers as they have to evaluate duplicative requirements and then implement the rules that are the most restrictive.

After considering these comments and discussing them with our legal counsel, I suggest that we amend this bill (see attached for suggested amendments) to only include sections relating to opting out of the health information network as the decision to opt in or opt out of a health information exchange are both acceptable

under the HIPAA Privacy Rule. Understandably, the sponsors of this bill felt that it was important enough to have this policy discussed by the Legislature and included in Century Code rather than having it included in administrative code as envisioned by section 54-59-26.2(d). I have attached the proposed administrative rules for your consideration since they are almost complete. These rules will need to be revised again for the changes that the Department of Health and Human Services just made to the HIPAA rules.

Currently, there are two major options that are being used around the United States for participation in a health information network. They are:

Opt out –an individual has determined that their information will not be disclosed by a health information organization, except as otherwise required by law. Their information is accessible to providers through the system until they have completed a form indicating they prefer not to have their information shared.

Opt in – an individual had indicated that they want their information in the health information exchange. No information is included in the exchange until they have completed a form to indicate they want their information in the system.

We have spent a lot of time discussing both options with HITAC members, domain workgroups and during our environmental scan when we were developing the strategic plan for the NDHIN. By and large, everyone felt that for North Dakota, the opt out method was the best method to use

Thank you for the opportunity to appear before you today, I would be happy to address any questions.

PROPOSED AMENDMENTS TO SENATE BILL NO. 2250

Page 1, remove lines 8 through 10

Page 1, line 12, after "54-59" remove "and any other entity that provides data transmission of protected"

Page 1, remove lines 13 through 23

Page 2, remove lines 1 through 16.

Page 2, replace lines 18 and 19 with "An individual may opt out of participating in a health information organization."

Page 2, remove lines 20 through 31

Page 3, remove lines 1 through 4

Page 3, line 10, replace "Completely opting" with "Opting" and after "organization" insert "except as required by law"

Page 3, remove lines 21 through 30

Page 4, remove lines 1 through 31

Page 5 remove lines 1 through 30

Page 6, remove lines 1 through 23

Renumber accordingly

Attachment #3

Title 112

INFORMATION TECHNOLOGY

Article
112-01 Reserved
112-02 North Dakota Health Information Network

ARTICLE 112-02

NORTH DAKOTA HEALTH INFORMATION NETWORK

ARTICLE 112-02
ORGANIZATION

Chapter
112-02-01 Organization

112-02-01. Organization of the Health Information Technology Office.

1. **History.** The sixty-first legislative assembly created the Health Information Technology Office in the Department of Information Technology and created the Health Information Technology Advisory Committee.

2. **Purpose.** The Health Information Technology Office, upon recommendations of the advisory committee, shall implement a statewide interoperable health information infrastructure, named the North Dakota Health Information Network (HDHIN), that is consistent with emerging national standards; promote the adoption and use of electronic health records and other health information technologies; promote interoperability of health information systems for the purpose of improving health care quality, patient safety, and the overall efficiency of health care and public health; apply for federal funds that may be available to assist the state and health care providers in implementing and improving health information technology; establish a health information technology loan program to provide loans to health care providers for the purpose of purchasing and upgrading certified electronic health record technology, training personnel in the use of such technology, and improving the secure electronic exchange of health information.

   The Health Information Advisory Committee shall collaborate with and make recommendations to the health information technology office. The health information technology advisory committee consists of the state chief information officer or the chief information officers designee, the state health officer or the state health officer's designee, the governor or the governor's designee, the executive director of the department of human services or the executive director's designee, the chairman of the house human services committee and the chairman of the senate human services committee or if either or both of them are unwilling or unable to serve then the chairman of the legislative management shall appoint a replacement who is a member of the same legislative chamber as the individual being replaced, and individuals appointed by the governor to represent a broad range of public and private health information technology stakeholders.

Inquiries. General inquiries regarding the North Dakota Health Information Technology Office should be addressed to:

North Dakota Health Information Technology Office
600 East Boulevard Avenue, Dept. 112
Bismarck, ND 58505-0100

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

Article 112-02

DEFINITIONS

Chapter
112-02-02 Definitions

112-02-02. Definitions. Unless specifically stated otherwise, the following terms shall mean the following throughout this title:

1. "Account" means an account within the trust established for a participant.

2. "Authorized user" means a person who is authorized by a participant to participate in the North Dakota health information network and includes health care practitioners, employees, contractors, agents, or health insurance portability and accountability act business associates of a participant. Those who may qualify as authorized users may be further defined in the North Dakota health information network policies and procedures.

3. "Breach" is an impermissible use or disclosure of protected health information that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected Individual.

4. "Business Associate" has the meaning set forth in 45 C.F.R. 160.103 and generally means a person (individual, corporation, partnership, government agency, etc.) who is not a member of the workforce of a covered entity that performs or assists in the performance of a function or activity involving the use or disclosure of protected health information of the covered entity.

5. "Individual" means a person who is the subject of protected health information (PHI) and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

6. "North Dakota Health Information Network (NDHIN)" means the North Dakota system to electronically exchange health care information between participants. The North Dakota Information Technology Department (ITD) is required by statute, N.D.C.C. § 54-59-26(b) to implement and administer a health information

exchange that utilizes information infrastructure and systems in a secure and cost-effective manner to facilitate the collection, storage, and transmission of health information.

7. "Opt Out" means that an individual has chosen to not participate in the North Dakota health information network. The individual's protected health information will not be available for use and disclosure through NDHIN except as required by law or as authorized by the individual in a medical emergency.

8. "Participant" includes any organization, health care practitioner or institution, health plan, or clearinghouse who has executed a written participation agreement and business associate agreement with North Dakota Health information network.

9. "Protected Health Information" (PHI) means individually identifiable health information (any oral or recorded information relating to the past, present, or future physical or mental health of an Individual; the provision of health care to the Individual; or the payment for health care) maintained by any medium and transmitted by electronic media or in any other form or medium.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

INDIVIDUAL PARTICIPATION

Chapter
112-02-03 Individual Participation

1. **Purpose.** The North Dakota health information network functions to provide for the electronic use and disclosure of a participating individual's protected health information by qualifying participants and their authorized users.

2. **Individual Participation**. Individual participation in the North Dakota health information network is voluntary. All individuals are considered to be participating until an individual has made a written decision to opt out of participation in the North Dakota health information network. Unless an individual elects to not participate, the individual's protected health information will be available through the North Dakota health information network for the purposes specified in section 112-02-05.

   An individual may choose not to participate completely or except for a medical emergency by completing and submitting the designated form to the North Dakota health information network.

   If an individual has chosen to not participate in the North Dakota health information network, then the individual's protected health information will not be available for use and disclosure except as required by law or as authorized by the individual in a medical emergency.

   An individual may change a prior election by completing and submitting the designated form to the North Dakota health information network.

3. **Individual Rights.**

   1. An individual has the right to opt out of participation in the North Dakota health information network.

   2. A participant may not withhold coverage or care from an individual nor may a health insurer deny an individual a health insurance benefit based solely on that individual's choice to opt out of participation in the North Dakota health information network.

3. An individual has the right to request an amendment of incorrect individually identifiable health information created by the North Dakota health information network. The health information network may review the request if it relates to information created by the network or may require health care providers participating in the North Dakota health information network to review the request for an amendment.

4. An individual has the right to request an accounting of disclosures made by the health information network as the term "disclosure" is defined by the Health Insurance Portability and Accountability Act Privacy Rule and the Health Information Technology for Economic and Clinical Health Act.

5. An individual has the right to request a copy of the individual's individually identifiable health information that is available through the health information network. The health information network may provide the health information directly to the individual or may require health care providers participating in the North Dakota health information network to provide access to individuals.

6. An individual has the right to be notified, pursuant to 45 Code of Federal Regulations part 164, subpart D, of a breach that affects the individual's individually identifiable health information.

7. An individual has the right to file a complaint pursuant to the North Dakota health information network policies and procedures.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

PARTICIPANTS

Chapter
112-02-04 Participant Participation

112-02-04. Participant Participation.

1. North Dakota health information network grants the rights to access the North Dakota health information network to participants and authorized users with a legitimate business need for purposes of treatment, obtaining payment for treatment, health care operations, to comply with public health reporting requirements, and as required by law.

2. **Participant Agreement Requirement.** Participants must execute a participation agreement with the North Dakota health information network prior to being granted access. Access and use of the North Dakota health information network is nontransferable by the participant.

3. **Responsibilities.** Participants shall identify all of its authorized users in accordance with the North Dakota health information network policies and procedures. The North Dakota health information network shall establish a unique identifier for each authorized user.

   a. Access to an individual's protected health information shall be based on the authorized user's job function and relationship to the individual according to policies and procedures established by the North Dakota health information network.

   b. Participants shall notify North Dakota health information network within twenty-four hours of any authorized user who by reason of termination of employment or otherwise is removed as an authorized user.

   c. Participants shall provide training for all of its authorized users consistent with the participant's and North Dakota health information network policies including privacy and security requirements.

   d. The participant may suspend, limit, or revoke the access authority of an authorized user on its own initiative upon a determination that the authorized user has not complied with the par icipant's or the North Dakota health information network's policies. The participant shall be responsible for informing the North Dakota health information network

immediately and in any case within twenty-four hours, of any revocation or suspension.

4. **Notification of breach.** Participants shall notify the North Dakota health information network of an actual or suspected breach in the most expedient time possible and without unreasonable delay following discovery but no later than established policies of the North Dakota health information network and pursuant to the Breach Notification Rule, 45 C.F.R. Part 164, Subpart D (Breach Notification Rule).

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

USE AND DISCLOSURE

Chapter
112-02-05 Use and Disclosure of Protected Health Information

112-02-05. Use and Disclosure of Protected Health Information.

1. **Approved Uses and Disclosures.** A participant may use and disclose the protected health information accessible in the North Dakota health information network only for the following purposes:

   a. treatment, payment, and health care operations;

   b. permitted uses described in the North Dakota health information policies and procedures;

   c. permitted uses described in the participation agreement; and

   d. as allowed under the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E (Privacy Rule).

2. Prohibited Uses and Disclosures. An individual's protected health information may not be used without the individual's consent by the Nor h Dakota health information network, participant or a business associate without the individual's authorization for any of the following purposes:

   a. uses prohibited by North Dakota health information network policies and procedures.

   b. uses prohibited by law including federal, state, or local laws, rules or regulations.

   c. comparative studies or by third parties.

   d. the sale or commercial use of protected health information.

3. **Audits.** North Dakota health information network is responsible for auditing the use of the health information network.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

FEES

Chapter
112-02-06 Fees

112-02-06. Fees. North Dakota health information network will notify all participants of its intent to begin charging or modifying fees for participation prior to the implementation of the change. If a participant objects to the fees or modification of the fees, the participant may terminate its agreement with written notification to the North Dakota health information network.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

ENFORCEMENT

Chapter
112-02-07 Enforcement

112-02-07. Enforcement.

1. The health information technology director may suspend or terminate the participation in the North Dakota health information network of any participant or authorized user.

2. The health information technology director, or designee, may provide written notice of suspension of a participant's access to the North Dakota health information network to all participants and may provide a written summary of the reasons for the suspension to the suspended participant. The participant may follow the necessary provisions for the appeal mechanisms of the North Dakota health information network's policies and procedures by responding to the suspension with a plan of correction or an objection to the suspension. The health information technology director shall review and either accept or reject the plan of correction.

   a. If the plan of correction is accepted, the health information technology director will, upon completion of the plan of correction, reinstate the participant's access to the North Dakota health information network.

   b. If the plan of correction is rejected, the participant may appeal the health information technology director's decision to the health information technology advisory committee for a final determination.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

ARTICLE 112-02

PRIVACY AND SECURITY

Chapter
112-02-08 Privacy and Security Protections

112-02-08. Privacy and Security Protections. Appropriate safeguards shall be used to prevent use or disclosure of protected health information other than permitted by the North Dakota health information network's polices, including appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity, and availability of protected health information through North Dakota health information network.

At a minimum, appropriate safeguards shall be those identified in the health insurance portability and accountability act security rule and other applicable federal and state standards.

North Dakota health information network will report to a participant any successful unauthorized access, use, disclosure, modification, or destruction of participant's electronic protected health information of which North Dakota health information network is aware.

History: Effective
General Authority: NDCC 28-32-02.1
Law Implemented: NDCC 28-32-02.1, NDCC 54-59-25, NDCC 54-59-26

Attachment #4

The Choice
is Yours

Participation is completely voluntary.

- By default, your medical information will be shared through the North Dakota Health Information Network.
- If at any time you do not want to participate or if you only want your information available in a medical emergency, complete and submit the designated form with your doctor or directly with the North Dakota Health Information Network.
- You will NOT be denied medical care if you decide not to share your medical records through the North Dakota Health Information Network. However, if you decide not to share your medical information, emergency room doctors and other medical professionals may not have access to your medical information when needed, which could be critical to saving your life.
- You may choose to share your information again at any time by completing and submitting the designated form with your doctor or directly with the North Dakota Health Information Network.

You Can Request
a Change

- To request a change or correction to the information in your medical record, contact your doctor.

Your Rights
Notice of Privacy Practices

- You have the right to receive the North Dakota Health Information Network's Notice of Privacy Practices in a timely manner.
- You have the right to opt out of participation in the North Dakota Health Information Network.
- Your doctor may NOT withhold coverage or care from you, nor may a health insurer deny you a health insurance benefit based solely on your choice to opt-out of or participate in the North Dakota Health Information Network.
- You have the right to request an amendment or a change to your medical information that you feel is incorrect.
- You have the right to request an accounting of disclosures, or to know who your medical information was shared with, as defined by the Health Insurance Portability and Accountability Act Privacy Rule and the Health Information Technology for Economic and Clinical Health Act.
- You have the right to request a copy of your medical information that is available through the health information network. The health information network may provide the health information directly to you, or may require your doctor, participating in the health information network, to provide access to you.
- You have the right to be notified, pursuant to 45 Code of Federal Regulations part 164, subpart D, of a breach that affects your medical information.
- You have the right to file a complaint, as defined in the North Dakota Health Information Network policies and procedures.

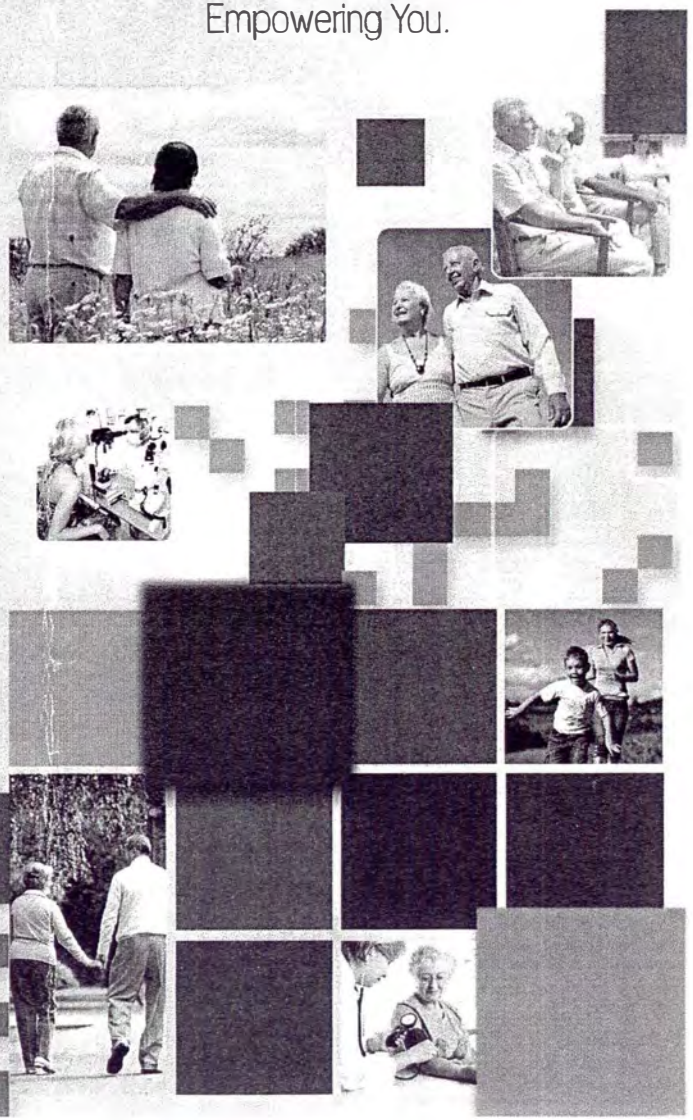
To review the complete NDHIN Privacy Practices, refer to the website below:

Contact us toll free at:
(855) 761-0534
www.ndhin.org/consumers

North Dakota Health Information Network
600 East Boulevard Avenue Dept. 112
Bismarck, ND 58505-0100

NDHIN
North Dakota Health Information Network

Improving Healthcare.
Empowering You.



What is the NDHIN?

The North Dakota Health Information Network (NDHIN) is a system created to securely share your health information by connecting your doctors' electronic medical record systems. Doctors need all of your health information to accurately diagnose and treat you. If they can view a more complete record of your health information, they can provide you with better care.

How will NDHIN help you?

- Improve coordination of your care by increasing availability of your medical records.
- Create safer administration of your prescription medications by allowing your doctor to see medication lists from multiple doctors.
- Reduce duplicate medical tests by granting your doctor access to your updated medical data.
- Empower your doctor to make more informed decisions by using your networked medical records.
- Avoid loss of key pieces of your medical record during unexpected events and disasters.

What information is shared with doctors?

- Your demographics, *such as* age, gender, location or marital status.
- Your reports, *such as* labs, x-rays, hospital admissions, discharges or transfers.
- Your medications, allergies and health problems.
- Your insurance information.
- Your advance directives.

We protect your information.

The NDHIN has security features in place to protect your medical information. Only authorized individuals will be able to view the shared data from your medical records.

We Have Your Best Interests at Heart

Your medical information may only be used or shared for:

Treatment, payment, and healthcare operations.

The permitted uses as described in the North Dakota Health Information Network Policies and Procedures and the Participation Network Agreement.

As allowed under the HIPAA Privacy Rule and state law.

Attachment #1

13.0187.04002
Title.

Prepared by the Legislative Council staff for
Senator Schaible
February 14, 2013

PROPOSED AMENDMENTS TO SENATE BILL NO. 2250

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact a new section to chapter 23-12 of the North Dakota Century Code, relating to participation in the health information organization.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new section to chapter 23-12 of the North Dakota Century Code is created and enacted as follows:

Voluntary participation in the health information organization - Prohibition on withholding care or benefits.

1. As used in this section:

   a. "Health information organization" means the health information exchange created under chapter 54-59.

   b. "Individually identifiable health information" has the meaning set forth in title 45, Code of Federal Regulations, section 160.103.

2. An individual may opt-out of participating in the health information organization by providing notice to the organization. If an individual chooses to opt-out of participating in the health information organization, the individual's individually identifiable health information may not be accessed by search by a health insurer, government health plan, or health care provider other than the provider who originally created or ordered the creation of the individually identifiable health information.

3. In opting out of participating in the health information organization under this section, the individual must have the option of:

   a. Opting out of participating; or

   b. Conditionally opting out, in which case the accessibility of the individual's individually identifiable health information is limited to access by a health care provider who determines access is required by a medical emergency.

4. An individual's decision to opt-out of participating in the health information organization:

   a. May be changed at any time by the individual by providing written notice to the health information organization.

   b. Does not prohibit use or disclosure of individually identifiable health information which is required by law.

5. A health care provider, health insurer, or government health plan may not withhold coverage or care from an individual nor may a health insurer deny an individual a health insurance benefit plan based solely on that individual's choice to participate or to opt-out of the health information organization."

Renumber accordingly

#1

Testimony on Senate Bill 2250

House Human Services Committee, March 19, 2013

Mr. Chairman, and members of the committee, I am Senator Margaret Sitte from District 35 in Bismarck.

Who has access to your personal medical records? Do most citizens even realize their medical records are becoming of a federal system of health care information? Do most people even realize each person in this county will have an Electronic Health Record by January 1, 2014? These questions are central to the SB 2250, a proposed new section of law to address privacy of medical records.

This bill is slim shadow of its original form. The bill was modeled on Arizona state law, and I spent many hours in many meetings with the Information Technology Department, the North Dakota Medical Association and Blue Cross/Blue Shield trying to achieve that broader policy. Unfortunately, much of that work fell apart in committee when those groups raised questions after I left the room.

This bill provides a simple opt-out of the health information exchange. Subsection 2 is the heart of the bill. If an individual chooses to opt out of the health information exchange, he or she may do so without repercussions. Opting out will not be cause for withholding care or benefits.

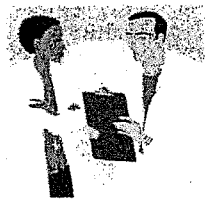
Hippocrates taught, "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."

This legislative assembly owes it to the citizens of North Dakota to ensure that they have as much privacy with their doctor as we can possibly secure for them. Hippocrates would remind us that privacy is a foundational principle of quality health care.

Please refer to Attachment 1, Inside the Fence

Attachment 2 is an Article in the Wall Street Journal by Dr. Peel

Attachment 3 demonstrates just how easy it is for "anonymized" information to be linked to a specific person.

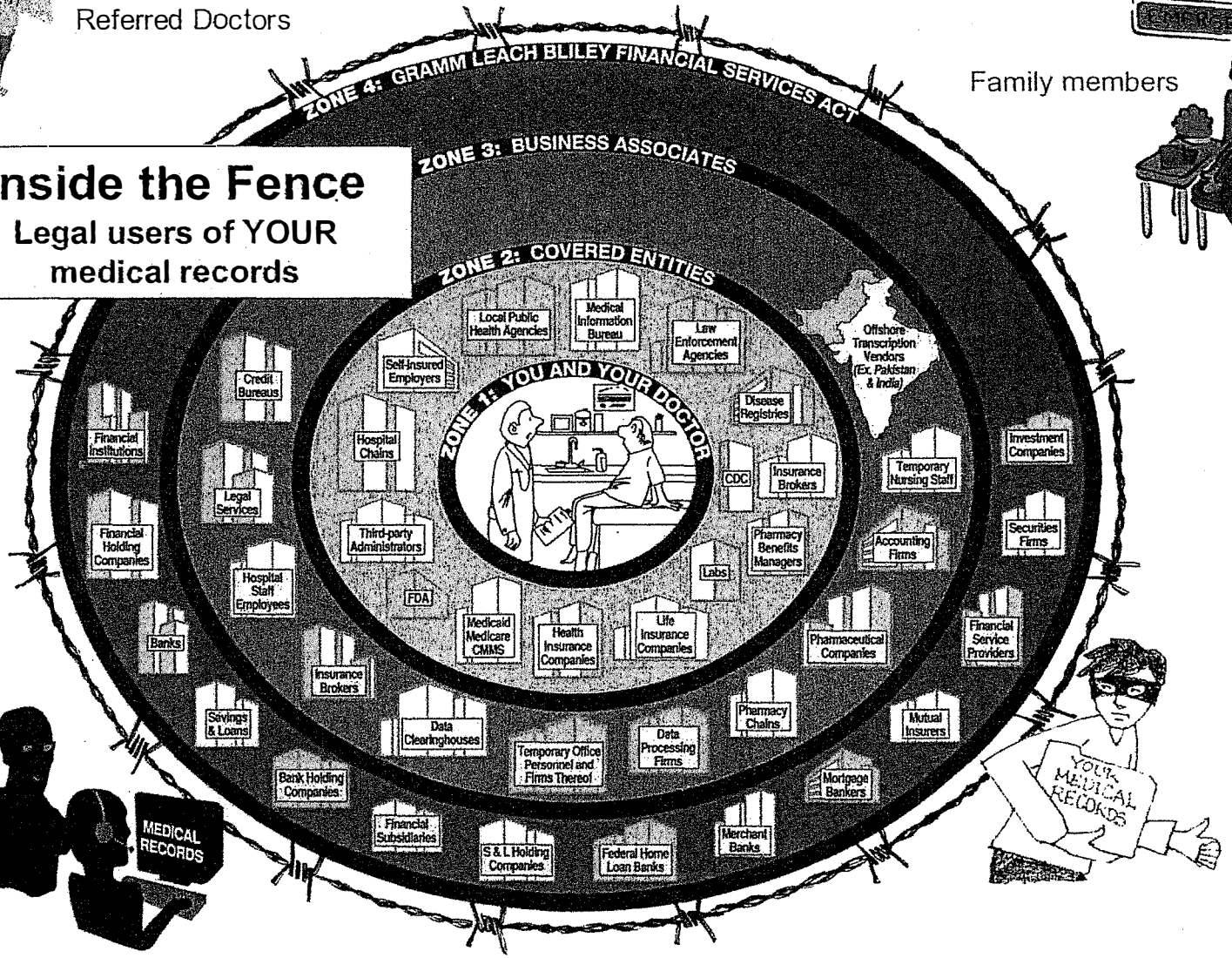


Referred Doctors

Family members

Inside the Fence

Legal users of YOUR medical records



www.patientprivacyrights.org

Attachment 1

Attachment 2

http://online.wsj.com/article/SB10001424052748703580904575132111888664060.html?mod=googlenews_wsj
Opinion Journal

THE WALL STREET JOURNAL
MARCH 23, 2010

Your Medical Records Aren't Secure

The president says electronic systems will reduce costs and improve quality, but they could undermine good care if people are afraid to confide in their doctors.

By DEBORAH C. PEEL

I learned about the lack of health privacy when I hung out my shingle as a psychiatrist. Patients asked if I could keep their records private if they paid for care themselves. They had lost jobs or reputations because what they said in the doctor's office didn't always stay in the doctor's office. That was 35 years ago, in the age of paper. In today's digital world the problem has only grown worse.

A patient's sensitive information should not be shared without his consent. But this is not the case now, as the country moves toward a system of electronic medical records. In 2002, under President George W. Bush, the right of a patient to control his most sensitive personal data—from prescriptions to DNA—was eliminated by federal regulators implementing the Health Information Portability and Accountability Act. Those privacy notices you sign in doctors' offices do not actually give you any control over your personal data; they merely describe how the data will be used and disclosed.

In a January 2009 speech, President Barack Obama said that his administration wants every American to have an electronic health record by 2014, and last year's stimulus bill allocated over $36 billion to build electronic record systems. Meanwhile, the Senate health-care bill just approved by the House of Representatives on Sunday requires certain kinds of research and reporting to be done using electronic health records. Electronic records, Mr. Obama said in his 2009 speech, "will cut waste, eliminate red tape and reduce the need to repeat expensive medical tests [and] save lives by reducing the deadly but preventable medical errors that pervade our health-care system."

But electronic medical records won't accomplish any of these goals if patients fear sharing information with doctors because they know it isn't private. When patients realize they can't control who sees their electronic health records, they will be far less likely to tell their doctors about drinking problems, feelings of depression, sexual problems, or exposure to sexually transmitted diseases. In 2005, a California Healthcare Foundation poll found that one in eight Americans avoided seeing a regular doctor, asked a doctor to alter a diagnosis, paid privately for a test, or avoided tests altogether due to privacy concerns.

Today our lab test results are disclosed to insurance companies before we even know the results. Prescriptions are data-mined by pharmacies, pharmaceutical technology

vendors, hospitals and are sold to insurers, drug companies, employers and others willing to pay for the information to use in making decisions about you, your job or your treatments, or for research. Self-insured employers can access employees' entire health records, including medications. And in the past five years, according to the nonprofit Privacy Rights Clearinghouse, more than 45 million electronic health records were either lost, stolen by insiders (hospital or government-agency employees, health IT vendors, etc.), or hacked from outside.

Electronic record systems that don't put patients in control of data or have inadequate security create huge opportunities for the theft, misuse and sale of personal health information. The public is aware of these problems. A 2009 poll conducted for National Public Radio, the Kaiser Family Foundation and the Harvard School of Public Health asked if people were confident their medical records would remain confidential if they were stored electronically and could be shared online. Fifty nine percent responded they were not confident.

The privacy of an electronic health record cannot be restored once the contents are sold or otherwise disclosed. Every person and family is only one expensive diagnosis, one prescription, or one lab test away from generations of discrimination.

The solution is to insist upon technologies that protect a patient's right to consent to share any personal data. A step in this direction is to demand that no federal stimulus dollars be used to develop electronic systems that do not have these technologies. Some argue that consent and privacy controls are impractical or prohibitively costly. But consent is ubiquitous in health care. Ask any physician if she would operate on a patient without informed consent.

There is no need to choose between the benefits of technology and our rights to health privacy. Technologies already exist that enable each person to choose what information he is willing to share and what must remain private. Consent must be built into electronic systems up front so we can each choose the levels of privacy and sharing we prefer.

My organization, Patient Privacy Rights, is starting a "Do Not Disclose" petition so Americans can inform Congress and the president they want to control who can see and use their medical records. We believe Congress should pass a law to build an online registry where individuals can express their preferences for sharing their health information or keeping it private. Such a registry, plus safety technologies for online records, will mean Americans can trust electronic health systems.

Privacy has been essential to the ethical practice of medicine since the time of Hippocrates in fifth century B.C. The success of health-care reform and electronic record systems requires the same foundation of informed consent patients have always had with paper records systems. But if we squander billions on a health-care system no one trusts, millions will seek treatment outside the system or not at all. The resulting data, filled with errors and omissions, will be worth less than the paper it isn't written on.

Attachment 3

http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

"Anonymized" data really isn't—and here's why not

Companies continue to store and sometimes release vast databases of " ...

by Nate Anderson - Sept 8 2009, 6:25am CDT

The Massachusetts Group Insurance Commission had a bright idea back in the mid-1990s—it decided to release "anonymized" data on state employees that showed every single hospital visit. The goal was to help researchers, and the state spent time removing all obvious identifiers such as name, address, and Social Security number. But a graduate student in computer science saw a chance to make a point about the limits of anonymization.

Latanya Sweeney requested a copy of the data and went to work on her "reidentification" quest. It didn't prove difficult. Law professor Paul Ohm describes Sweeney's work:

At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. In a theatrical flourish, Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office.

Boom! But it was only an early mile marker in Sweeney's career; in 2000, she showed that 87 percent of all Americans could be uniquely identified using only three bits of information: ZIP code, birthdate, and sex.

Such work by computer scientists over the last fifteen years has shown a serious flaw in the basic idea behind "personal information": almost all information can be "personal" when combined with enough other relevant bits of data.

That's the claim advanced by Ohm in his lengthy new paper on "the surprising failure of anonymization." As increasing amounts of information on all of us are collected and disseminated online, scrubbing data just isn't enough to keep our individual "databases of ruin" out of the hands of the police, political enemies, nosy neighbors, friends, and spies.

If that doesn't sound scary, just think about your own secrets, large and small—those films you watched, those items you searched for, those pills you took, those forum posts you made. The power of reidentifiation brings them closer to public exposure every day. So, in a world where the PII concept is dying, how *should* we start thinking about data privacy and security?

Don't ruin me

For almost every person on earth, there is at least one fact about them stored in a computer database that an adversary could use to blackmail, discriminate against, harass, or steal the identity of him or her. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm.

Examples of the anonymization failures aren't hard to find.

When AOL researchers released a massive dataset of search queries, they first "anonymized" the data by scrubbing user IDs and IP addresses. When Netflix made a huge database of movie recommendations available for study, it spent time doing the same thing. Despite scrubbing the obviously identifiable information from the data, computer scientists were able to identify individual users in both datasets. (The Netflix team then moved on to Twitter users.)

In AOL's case, the problem was that user IDs were scrubbed but were replaced with a number that uniquely identified each user. This seemed like a good idea at the time, since it allowed researchers using the data to see the complete list of a person's search queries, but it also created problems; those complete lists of search queries were so thorough that individuals could be tracked down simply based on what they had searched for. As Ohm notes, this illustrates a central reality of data collection: "data can either be useful or perfectly anonymous but never both."

The Netflix case illustrates another principle, which is that the data itself might seem anonymous, but when paired with other existing data, reidentification becomes possible. A pair of computer scientists famously proved this point by combing movie recommendations found on the Internet Movie Database with the Netflix data, and they learned that people could quite easily be picked from the Netflix data.

Such results are obviously problematic in a world where Google retains data for years, "anonymizing" it after a certain amount of time but showing reticence to fully delete it. "Reidentification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization," Ohm writes. "This is no small faith, for technologists rely on it to justify sharing data indiscriminately and storing data perpetually, all while promising their users (and the world) that they are protecting privacy. Advances in reidentification expose these promises as too often illusory."

For users, the prospect of some secret leaking to the public grows as databases proliferate. Here is Ohm's nightmare scenario: "For almost every person on earth, there is at least one fact about them stored in a computer database that an adversary could use to blackmail, discriminate against, harass, or steal the identity of him or her. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm. Perhaps it is a fact about past conduct, health, or family shame. For almost every one of us, then, we can assume a hypothetical 'database of ruin,' the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given access to it to our worst enemies."

Because most data privacy laws focus on restricting personally identifiable information (PII), most data privacy laws need to be rethought. And there won't be any magic bullet;

the measures that are taken will increase privacy or reduce the utility of data, but there will be no way to guarantee maximal usefulness and maximal privacy at the same time.

There are approaches that can reduce problems. Instead of releasing these huge anonymized databases, for instance, make them interactive, or have them report most results in the aggregate. (But such techniques sharply limit the usefulness of the data.)

Ohm's alternative is an admittedly messier system, one that can't be covered with simple blanket laws against recording Social Security numbers or releasing people's name and addresses. Such an approach has failed, and now looks like playing "Whac-A-Mole" with personal data. "The trouble is that PII is an ever-expanding category, writes Ohm. "Ten years ago, almost nobody would have categorized movie ratings and search queries as PII, and as a result, no law or regulation did either." Expanding privacy rules each time some new reidentification technique emerges would be unworkable.

Instead, regulators will need to exercise more judgment, weighing harm against benefits, and the rules may turn out to be different for crucial systems like healthcare. At the same time, the US needs comprehensive legislation on data privacy to set a minimum threshold for all databases, since Netflix, AOL, and others have made clear that we have no real idea in advance which pieces of seemingly harmless data will turn out to identify us and our secrets.

#2

TESTIMONY BEFORE THE HOUSE
HUMAN SERVICES COMMITTEE
SENATE BILL 2250
MARCH 19, 2013

Mr. Chairman, members of the committee, I am Sheldon Wolf, the ND Health Information Technology Director. I am here today to provide information on Senate Bill 2250 on behalf of the Health information Technology (HIT) Office and the Health Information Technology Advisory Committee (HITAC).

This bill relates to the option that an individual has regarding participation in the North Dakota Health Information Network (NDHIN). Currently, there are two major options that are being used around the United States for participation in a health information network. They are:

Opt out – an individual has determined that their information will not be disclosed by a health information organization, except as otherwise required by law. Their information is query able to providers through the system until they have completed a form indicating they prefer not to have their information shared.

Opt in – an individual has completed a form which indicates they want their information in the health information exchange. No information is query able through the exchange until the individual has completed a form indicating their participation.

We have spent a considerable amount of time discussing both options with HITAC members, domain workgroups and during our environmental scan when we were

developing the strategic plan for the NDHIN. By and large, everyone felt the opt out method was the best method to use in North Dakota.

Section 1.3 of the bill gives an individual three options of participating in a health information exchange. The first option allows an individual to opt of participating in the NDHIN. If they select this option, the individual's identifiable health information may not be accessed by search by a health insurer, government health plan, or healthcare provider other than the provider who originally created or ordered the creation of the individually identifiable health information.

The second option allows an individual to conditionally opt out. In this case their information is not available for search, like the first option. However, if a health care provider determines access is required because of a medical emergency, the health care provider can "break the glass" and search for the information. The third option, which is the default option, allows the individually identifiable health information on an individual to be searchable by a provider.

Thank you for the opportunity to appear before you today, I would be happy to address any questions.