FTC SENIOR ID THEFT WORKSHOP
MAY 7, 2013
TRANSCRIPT
SEGMENT 2

MEGAN COX: Good morning. I'm Megan Cox, and I'm an attorney with the Division of Privacy and Identity Protection here at the Federal Trade Commission. And this morning, our panel is here to discuss the issue of medical identity theft and seniors. And we are defining this issue broadly, for the purposes of this panel, as the fraudulent use of another's personally identifiable information to commit health care fraud. And Personally Identifiable Information, also known as PII, could be a name, social security number, or protected health information. And this fraud often involves a thief obtaining medical goods and services, or the thief making false claims for medical goods or services.

And this topic is relevant to older Americans, as they often interact with the health care system with a greater frequency, and have more points of contact with the health care system overall. And so have more information circulating widely about them.

This issue is a complex one because big payments and disbursed information can hide the problem of medical identity theft. And often, there are sophisticated perpetrators operating in the field of medical identity theft.

Furthermore, the usual avenues through which one detects that they have been a victim of identity theft generally do not work with the issue of medical identity theft specifically. So today, we're going to talk about these topics with our knowledgeable panelists. We're going to talk about the scope of the problem for seniors, causes of the problem, prevention and detection, and steps to mitigate the risks for older Americans.

And then, we'll take audience questions. So if you have those note cards in your folder, you can fill them out as the panel progresses.

And on our panel today, we have Pam Dixon from the World Privacy Forum, Andy McKee from Health and Human Services Office of Inspector General, Rick Kam with ID Experts, and Robin Slade of the Medical Identity Fraud Alliance. So thank you all for joining us here today.

And Robin, if we can start with you. Can you give us a better working definition of what medical identity theft is and how seniors are vulnerable?

ROBIN SLADE: Right. Well, medical identity theft, it occurs when someone uses another's information to receive medical-related services, to buy drugs or to unlawfully gain financial benefits such as fraudulently billing insurance companies or Medicare for services that were never performed.

I think it's important to understand though, that medical identity fraud can happen with or without the person's consent. Someone may lend their insurance to another to get services and

not understand the devastating consequences that could be attached to that. But often, it occurs with no fault at all of the person who's become victimized.

With financial identity theft, the individual is usually made whole by their financial institution for-- at least for the loss of the funds. But medical identity theft, the results can interfere with your care. And it could, potentially, kill you.

What happens if your blood type is mixed with that of the perpetrator? What happens if you're rushed to the hospital with an appendicitis and your appendix has already-- the individual who's stolen your identity, their appendix has already been removed. So clearly, the issues go far beyond financial loss.

And when it comes to seniors, what makes them particularly vulnerable is that they tend to be the preferred targets for fraudsters for various types of crime and scams. And because of these fraudsters, and also unscrupulous relatives, caregivers, often see these individuals as being vulnerable. And perhaps, more trusting or less financially sophisticated than others. That's what tends to make them a target.

MEGAN COX: OK. Thank you. And Pam, could you elaborate on the correlation between age and medical identity theft, and what the World Privacy Forum found in its report?

PAM DIXON: OK. So just to level set very quickly-- sorry for booming. OK, so in 2005, I was asked to testify before the NCBHS, and I was asked to look for what risks existed in electronic health care files and the potential risks in any kind of exchange of digital health files.

And I was sitting at my desk and it just occurred to me, I wonder if there is identity theft in health care to the extent to which there is in the financial sector? And I started looking. I googled medical ID theft and nothing was there.

And then, I went on to the court systems and started looking for cases and found literally hundreds of cases. So I wrote the first report on medical identity theft-- coined the term-- and pushed for a lot of the medical data breach laws that are in existence now.

Since 2005, I've been continuing to do research in this area. And there are two things that have become quite apparent in the research. And I was telling Megan, I have about 4,000 pages of raw research in my head and I'm very happy to share it with you. If I don't answer all of your questions, please do send us an email or check our medical identity theft page. The resources are free and they are consumer tested. So let me focus on the senior aspect of the crime.

There is a very substantial geographic component to medical identity theft. The geographical component, we have unambiguously been able to correlate also to Medicare/Medicaid distribution lines. So for example, you're going to find high instances of medical forms of identity theft in Florida, Houston, Southern California, Northern California, all the places you might expect to find high instances of Medicare/Medicaid fraud.

There's also a little blip that we find in Michigan thanks to one particularly inventive and resourceful kind of fraud ring. But in general, that is a huge, huge risk factor for seniors.

If you live in Fargo, North Dakota, your chances of becoming a medical identity theft victim are substantially lower than if you live in one of these kind of hot spot areas. So that's first.

But secondly, just by virtue of being a senior, you have increased risk for a number of reasons.

Number one, you are already in the health care system. Number two, a lot of elderly are also elderly poor. And this isn't something I've really heard discussed today, but the elderly poor are a very significant aspect of the victimization of seniors here because they really need a lot of access to service. And then, the elderly disabled are also a big subset here.

And so I don't have time to go into the key patterns of this crime on this question, but one of the things that really comes into play that victimizes seniors in particular is the way that free food, free transportation, and free medical exams are mass marketed to seniors and offered fraudulently under Medicare/Medicaid guidelines.

So for example, seniors will be offered-- we will take you to and from your appointment for free, even if you're ambulatory. Which is, of course, a big no-no. But this will really rake people in. And then, what do they? They just take a nice photocopy of their card, their government services card, and they're off and running a lot of times. So there's a lot more depth to this than I've just indicated, but that's a start.

There was a question on the last panel-- we don't hear, someone said seniors don't have that much identity theft. OK, so financial forms of the crime-- maybe I'll buy that a little bit. But let me tell you, medical identity theft? Seniors are a primary target. And this crime has profound consequences for seniors and for their loved ones. So this is certainly worthy of focus.

MEGAN COX: Thank you.

Andy, maybe you can collaborate. So Pam mentioned the free medical services. What types of medical ID theft will seniors be more susceptible to, Medicare fraud or health care product scams, stolen health information?

ANDY MCKEE: Right. And just as a little bit of background, I work for Health and Human Services OID, so we investigate Medicare and fraud issues and Medicare and Medicaid fraud cases. So that's what I can speak to. But Pam was right on the money, we continuously see Medicare beneficiaries who are targeted by telemarketers. We call them recruiters. They're called recruiters in different parts of the country. They're called cappers out on the West Coast.

And basically, what they do is they'll drive around and say, do you need a wheelchair? Come see us and we'll give you some free groceries, or we'll give you $100, or we'll give you something for free.

And the scary thing is a lot of people don't realize or-- well, I guess most seniors realize this. But your Medicare number is simply your social security number with an alphanumeric digit at the end of it or at the beginning in some cases. So once that number becomes compromised, it's compromised. You can't put the genie back in the bottle. You can't get it back. The government's not going to issue you another one. So once that number gets compromised, it can be used over and over again.

I was a case agent down in Florida. I can tell you, I've worked a case down there that involved identity theft where Medicare patients' information was stolen. Their Medicare numbers were stolen. The case involved activity that occurred in 2006.

One of the Medicare beneficiaries had died in 1988. They weren't getting paid for this. There's no quality control for people who steal Medicare numbers or who have numbers that are compromised, so they didn't know that this person had died in 1988. They just kept billing for it. They weren't getting paid for it, but it just gets passed among different criminal groups. So just an example of how those numbers kind of get passed around.

And as Pam mentioned as well earlier, they are criminals. They are a criminal element. They target the most vulnerable among us. And oftentimes, that people who receive Medicare and Medicaid. Medicare is paid for people who are elderly or disabled. Oftentimes, they may have some type of cognitive issue as they're getting older. A lot of times we'll see people's identities that are stolen while they're in an assisted living facility. They don't even know that their identity has been stolen. So they're the most vulnerable among us.

From an agent perspective, that's horrible because the program is set up to protect them. And the criminals among us take advantage of that.

MEGAN COX: And Rick, maybe you can talk at a macro-level about what the Ponemon Institute has been studying about breaches of health care, and how that's been putting people at risk?

RICK KAM: Sure, Megan. Maybe just as a little way of background, what I'll be able to speak to is essentially some of the research that's been done around medical identity theft specifically, but also identity theft in particular. And let me start by first saying a couple things around the research about identity theft so we have a basic understanding of that.

The American National Standards Institute, a few years ago, started a series of projects around identity theft. They set up a standards panel. Some of the people I see in the audience are actually part of that panel. And the idea was to get a better understanding of really what the problem was, so that you can actually apply resources to deal with the problem. Whether you're in the federal government or state agencies or in private industry.

And what we found was, for other forms of identity theft, in particular financial identity theft very specifically, there's quite a bit of research. In fact, there are 180 research projects done that we identified with the ANSI project backed about five years ago.

When you look at medical identity theft in particular, there are very few projects or research projects done. And at this point in time, back in 2005, I think Pam Dixon was one of the few people that identified that this was a real problem. And so relative to the work that's been done to identify what this issue is, what impact it has on individuals, there really is now starting new projects to look at this.

So the Ponemon Institute-- I don't know if you folks know much about Dr. Larry Ponemon, but he's been in the industry of researching data breach issues over the last 10 years. In fact, he's probably one of the most published institutions around this particular topic.

Three years ago, he started to look at medical identity theft in particular, and patient privacy and data security issues. And so we had the opportunity to work with Dr. Ponemon three years ago to start to look at and understand what was causing not only medical identity theft. But more specifically, access to the information that is the cause of medical identity theft. Specifically, health insurance information, PII forms of protected health information, other things that were really the root cause of the problem.

And so the third year that the study was done and published was last year in December. So we had the opportunity to look at trends over the last three years. And what we found essentially was this--

Over the last three years, essentially organizations that were part of this benchmark study saw-- 94% of them saw a breach of protected health information, which includes not only name, address, social security number, but also things like your health insurance numbers, diagnosis, prescriptions, that kind of information. 94% of organizations experienced a breach of some significance over the last 2 years.

That means in the US, where there are approximately 300,000 covered entities-- hospitals and so forth-- 94% of them had a breach of significance over the last 2 years. 45% of those organizations had 5 or more breaches of protected health information. So the trend that we were seeing in this particular study was not only was this happening, but it was happening with increasing frequency across the industry.

So the question became, why is this? And what we start to discover through the research is there is an economic value to bad actors essentially to misuse this data for a variety of reasons. Medical identity theft being one of the forms of misuse, but all forms of identity theft, actually, based on the information that's being lost and stolen.

So that's just a little bit of the beginning of this. I can talk forever, so--

MEGAN COX: OK. And Pam, did you want to chime in on what the value of the health information is?

PAM DIXON: Yeah. I'd like to just maneuver just a little bit and refocus very slightly. I just wanted to compare and contrast two cases.

So it is so profitable to commit this crime. It is just luxurious. If you want to be a criminal, you may as well do this. Because it is a heinously profitable crime. And the profit comes at the expense of the most vulnerable people. It is just hideous to research, I have to tell you. That's a blanket statement.

In knowing these cases, let me share with you. This crime does not operate like the rest-- medical identity theft, there's a continuum.

When I wrote that first report in 2006, I was trying to prove that the crime existed because nothing had been written before. But now, I'm trying to really show where the continuum is.

OK, so in the case of seniors and how they're victimized, it's different than a younger person who may be actually victimized through a breach, which does happen, by the way-- and a lot. The way seniors can be victimized is slightly different because they have something that most other people don't. They have their SSN right on their Medicare card. And that is a huge, huge problem for them and a huge risk factor, which cannot be underscored enough.

So for example, there is a case in US v. Usman where 18 patients-- just 18 dialysis patients-- this guy billed over $3 million for 18 patients. He didn't need a data breach, all he needed was a photocopier. And this is a really important distinguishing feature.

Now, in another really heinous case in US v. Scott and Collie. What happened is that these folks went to the Emory Cancer Center and they purchased from an employee some prescription pads. And then they billed Medicare a million dollars for chemotherapy drugs. And then sold them back to Kroger's and some other legitimate pharmacies. This is how they made money.

And the other thing that they purchased was a small list of Georgia Medicare recipients that had been photocopied. Their name, their SNN, and that's it. So it can be a face crime where you have a few victims or it can be a faceless crime where you have a few more victims, but you can bill very high amounts of money for very few victims. And especially if you conduct the crime over time. So this crime does operate a little differently for seniors.

MEGAN COX: And could you-- and maybe Rick as well-- anticipate how or make your best guess for how you think the Affordable Care Act is going to impact? This with greater access to health care, there will be fewer people needing to commit this crime or is that not the case?

PAM DIXON: The criminals will always feel a need to commit this crime.

RICK KAM: Yeah, I think the issue is not necessarily that more people will have access to health care, but there will be more information essentially being stored in electronic health record systems. And this is an interesting aspect in terms of a game changer if you will, in terms of where health information exists.

It turns out in the old days, a few years ago, if you walked into your doctor's office or your health care provider's office, most of this information was in manila folders. In some cases-- I

remember in my dentist's office, they have it hanging in the reception area on the walls, accessible, basically, to everybody who's in the office.

Today, with-- and not only the Affordable Care Act, but the stimulus bill putting major incentives to drive everybody in health care to electronic health care record systems, you can literally store millions of records on a thumb drive.

And many of the breaches that have occurred of information have been because either a laptop that's been unencrypted has tens of thousands of records on them or a system, like the Veterans Administration had compromised, were-- what was it, close to 20 million some-odd veterans information was on that system. It's all consolidated now in these electronic health records which, makes it very easy to steal many, many individuals' information. So I think there's going to be more, unfortunately, breaches of this type.

MEGAN COX: Thank you. Robin, would you want to talk about some of the various stakeholders on this issue, and maybe what industry is feeling is the impact from it all?

ROBIN SLADE: Sure. I think the entire health care ecosystem is victimized and struggles to find assistance in how to resolve these issues. Individuals clearly are impacted. And if not directly, then indirectly. Those consumers whose identities have been stolen clearly are greatly impacted. But consumers are also impacted through increased insurance premiums and deductibles. I think we all agree that they have a right to the privacy and security of their protected health information.

From the industry level, with the Medical Identity Fraud Alliance, we're a health care consortium which is launching this summer. And our members are the stakeholders within the health care industry that are needed to develop the technology, the best practices, and the policies necessary to work towards lessening the exposure of patient data.

Yeah, that's going to take a coordinated effort. It's going to include everybody that touches the data and everybody that's necessary in order to help stop the fraud. So those stakeholders will include the health insurance plans, the providers, the technology service providers, law enforcement, government agencies, and other industry organizations.

I look at health care's move towards electronifying the records as-- I equate it with what financial services went through in the advent of e-commerce. I see a lot of similarities in trying to understand how to protect that data and what to do. So I think we have an opportunity to get the right people together at the table and talk about what those policies and procedures should be. And I think we also have the opportunity to leverage a lot of what financial services did as well.

I think there is a direct correlation-- often, if an individual becomes a victim of medical identity fraud, they also become a victim of financial Identity fraud, and vice-versa. So I think that those two industries do need to work together in order to help resolve some of the issues.

MEGAN COX: And another large stakeholder is the government. So Andy, would you want to comment on the impact on the government at the federal level? And Pam, if you want to talk about the states?

ANDY MCKEE: Sure. Not to be trite about it, but my grandmother used to always say there's no such thing as a free lunch. And that's what we see. Medicare beneficiaries will often say, well, the government's paying for this. I don't have to pay the copay. Nobody's trying to collect the copay from me.

But at the end of the day, the money comes from the taxpayer. And it comes from all of us, all the Medicare premiums that we pay. In this time of fiscal austerity, the billions and billions that are lost to fraudulent Medicare billings is horrendous.

And the lines between government and industry get blurred quite a bit, I would think. They do get blurred quite a bit when we're talking about Medicare billing because you have Medicare HMOs that are managed care programs, and they get paid a certain amount to administer Medicare HMOs. So who's the victim? Is it the government because the government eventually pays for it? Or is it the private industry that's administering the plan because they're victimized as well?

So we continue to see instances where-- and we're getting better at it as federal law enforcement is sharing intelligence and sharing information with the private side. Because a lot of times they'll be seeing something that's impacting them and we'll say, hey, it's impacting Medicare's as well. So there are initiatives in place to try to share that information. But again, those lines get blurred between the government and private industry as well.

PAM DIXON: I think it's going to be incredibly important to look in the right place to solve the problems that are associated with this crime.

So if we look in the wrong places and we point the fingers at the wrong people and put the wrong solutions in place, the crime will continue unabated. So a very good example of this is what I call TSA patient screening. So in almost every case of senior medical identity theft-- not other cases, but in seniors, it is-- I don't actually know of a case. You may, but I don't actually know of a case where a licensed physician was not involved. I don't.

There are a few where maybe the physician ID was stolen or the signature was forged. But usually, there is some complicity and some cooperation among health care stakeholders. And I'm really focused on the senior forms of the crime.

In the broader issue of medical identity theft, there is a striation. There is a continuum. And there can be cases where there is not complicity, particularly in the case of health care data breach.

However, seniors-- different. And it's going to be incredibly important to understand that in order to resolve the problems associated with medical identity theft for seniors, that the health care institutions and the health care stakeholders are going to have to be involved at the state and federal level, and private and public. And without that, it's not going to get resolved.

One thing that I must mention is incredibly important is-- number one, every time a senior goes to get health care, they're going to be asked for their card. It's going to be digitized or photocopied or scanned, whatever. That's a big risk right there. That's something that has to be looked at in terms of senior identity theft.

The second thing, though, is that the Federal Trade Commission worked very hard to pass red flag rules for the health care industry. That didn't work out so well, the AMA, famously, sued and managed to get themselves free of that.

What would have happened though, is that the health care industry would have had some minimal requirements for having some identity theft flags and markers and deterrents in place. And I think that that's still a really good idea for the industry to do voluntarily because I think this problem's going to have to be fixed from the inside out, not the outside in.

And I'm a little concerned about-- I'm making direct parallels with the financial sector. There are cases where it's very helpful to do this, particularly in cases of breach where you can bring in some technologies and whatnot that are very, very helpful. But in the case of seniors, it's a little bit different. And we've got to be really careful that we don't try to rely on technologies too much to solve a problem that is fundamentally social in its nature. And therefore, very rascally and very challenging to solve.

OK, so the same doctor who's falsifying the health care files under HIPAA is the same doctor who has to correct those files.

There was a case in Boston, a very famous one with a psychologist. The guy refused to fix his patients' file. Some of those patients wouldn't and couldn't get employment or benefits because they had reached their insurance caps and all sorts of other ungodly things. So we've got to be really careful to look at those really systemic, stubborn, ingrained in the law kinds of problems.

MEGAN COX: Thank you. So now we're going to move more onto prevention and detection of the issue. And as you said, it can be very rascally. So detecting it can be an issue.

Andy, what have you seen about how the problem has come about, and how people have realized it's a problem in their life?

ANDY MCKEE: Sure. Identities are stolen several ways. First of all, like we're talking about-- data breaches. We continue to see cases where information is stolen. Sometimes it's from a hacker who gets into a system. And we tend to see that a lot, quite honestly, with organized criminal cases. Organized criminal groups tend to have a really strong cyber component. They're actually experts at penetrating systems. So health care systems are particularly vulnerable and particularly attractive to them because of how much money you can make.

As Pam was mentioning, 18 beneficiaries netted $3 million. So if you're a bad guy and you're looking at somewhere to steal-- hey, this is a pretty lucrative place to look.

But outside of data breaches, I'll touch briefly on electronic health records. I think they cut both ways. As far from an investigative standpoint, they're great because anybody who accesses an electronic health record, they leave a footprint. We go in to look and say, hey, who accessed these records? We can find out exactly who did it and when they accessed them. So in that way, they're good.

But in the same way that they improve efficiency and effectiveness for the provider, for the criminal they also-- they don't really care if they're caught. They don't really care. If they're a hacker, they can get in and get them as well.

We continue to see cases where identities are simply photocopied. Somebody goes into somebody's medical record, photocopy their Medicare number or their social security number, and then they stick it in their pocket and walk out.

We've seen cases where someone will-- a home health care aid will go in-- or somebody working in an assisted living facility, they'll have a cell phone with them and they'll just simply text out somebody's social security number. It's very easy, very simple, almost impossible to catch.

And we continue to see one-off identity theft as well, where a family member may steal somebody's identity, sell it to somebody they know. Medicare numbers go, depending on what part of the country, anywhere from $10 to $100 a piece.

And unfortunately, we see cases as well where Medicare beneficiaries may sell their information. Especially in some of the really high fraud areas. Unfortunately, it's very lucrative to be-- we call them a professional patient, where you sell your Medicare benefits.

I don't really need infusion services, but they're going to pay me $300 this month. Hey, here's my Medicare number. You can bill for it. So we continue to see cases that-- as well we continue to see an increase in telemarketing schemes, where people will call Medicare beneficiaries and say, I'm from Medicare. Can you verify your Medicare number for me? And the Medicare beneficiary will give them their Medicare number.

Or, you've got a grant from HHS. All I need is your social security number and your bank account information and I can wire the money to you. And oftentimes, they'll give up their bank account information or other type of information. So telemarketing, especially with diabetic supplies, we continue to see that to be problematic. Where, again, they'll say, are you a diabetic? Do you need test strips? We'll send you these test strips and they'll be free for you.

They'll start off with the diabetic test strips, and then soon the Medicare beneficiary starts receiving a heating pad, orthodontics and prosthetic devices, whether they need them or not. And the diabetic supplies are simply the entryway drug for lack of a better term, and then they continue to bill. And again, once that number is compromised, it's compromised.

MEGAN COX: Thank you. So Robin, in light of those stories, what are the best ways for seniors to prevent medical ID theft? And what can seniors do about the fact that their SSN is their Medicare number?

ROBIN SLADE: Often, it's of no fault of the senior when medical identity theft occurs. But what I would say is protect your information, your health-related information just like you would your financial-related information. Keep your health and credit-related personal information completely confidential. Keep it in a safe, locked place.

Leave your insurance cards at home and carry a copy of your insurance card. You can black out all but the last few digits. So that can help. But also, make sure that-- what I recommend is that you keep a calendar of the services that you've had. So if you visit your doctor, you can log it in.

And then, when your explanation of benefits comes in or your Medicare summary notice, check it against that calendar. Make sure that the dates line up. Are these actually services you may have had? And if you don't know, call the office to find out. Because often, as you know, the explanation of benefits are difficult to read.

Watch for unsolicited credit card offers or bills. And make sure that you get your credit reports periodically. At least annually, which you can do free, which the last panel mentioned.

Consumers are entitled to one free credit report annually from each of the credit bureaus, so make sure you check those. Because often, they can uncover a bigger issue. So those would be some of the things that I would recommend.

MEGAN COX: Thank you.

PAM DIXON: I think something really important to add onto that list is when we do senior privacy training, which we do locally in San Diego-- that's where we're based-- we really hammer on the issue of free. If you see something for free-- a free exam, a free clinic, free food, or free transportation all in exchange for your Medicare card or Medicaid card, you've got to watch out. Because a lot of times those are scams.

As part of our research into our reporting on this issue, we just did a nationwide survey for free mass marketing. And we found so many scams that way. It was like picking fruit off of a tree.

And if you call them, they're the seniors. They're after this information. So really, really education around free is incredibly important.

And the telemarketing issue is very disturbing and hard to handle because it's reaching seniors who have cellphones right there. And it's really hard to intervene when there's a social situation and someone really slick.

MEGAN COX: And branching off of that, should seniors engage in web-based applications? Now that people have cell phones and smartphones, should they engage in health care communications with doctors through mobile apps? Do you have any insights?

PAM DIXON: Email is the number one technology that's used by seniors. And that's the number two thing they're doing, is looking at news and whatnot. And the number three that we found, at

least from our survey and actually interviewing seniors, is they're also looking at those genealogy websites, which I never would have predicted if we hadn't done the research. It was interesting.

And it was surprising, the seniors that we've interviewed have actually been wary of contacting and doing things online. So I think that's a very intriguing finding. I actually would've thought that there would have been more vulnerability there. But it seems to be that in person and telemarketing and through free ads, things for free, is much more effective for seniors at this point.

MEGAN COX: And moving into detection more. When people are looking at their explanation of benefits-- Andy, maybe you could comment about what they should be looking for?

ANDY MCKEE: Sure. And I think Robin touched on it as well. Just look for charges that don't look familiar. You didn't get a wheelchair and then suddenly there's a wheelchair on your explanation of benefits. You're not sure what a service-- you were in the hospital and there's a charge for something you didn't receive.

Look on there. If you have questions, there are numbers on your explanation of benefits where you can call and get help. There's a 1-800-Medicare number on there as well. You can contact that number and they can walk you through your EOB, your Explanation of Benefits, and tell you specifically what is being charged to Medicare.

And also, be on the lookout for someone trying to collect co-payments from you. If they say, hey, you owe us the 20%. Medicare's an 80/20 program. You owe us 20% for this wheelchair. You never received it. Be on the lookout for those types of things.

PAM DIXON: Something that occurs to me is some of the best criminals are experts at gilding the lily in such a way that even if you're looking at all this, sometimes you can't see it. Especially if there is a senior who, perhaps, has a memory issue or dementia and they have medical power of attorney somewhere else.

A senior can be getting, for example, dialysis care. And the lily can be gilded with the transportation services for that senior. And the person would never know. It would look completely legit to an outsider. So this is very challenging for the victim to find. It can really hide. This is a crime that hides very effectively.

And I want to make sure we don't blame seniors for not finding it because it's very hard to detect.

MEGAN COX: And are they always entitled to an itemized bill?

ANDY MCKEE: Yes. It will always show up on their explanation of benefits. It will detail every charge that was issued to Medicare under their Medicare number.

MEGAN COX: OK. And Rick, maybe we can talk about now breach notifications and how effective those are from data breaches?

RICK KAM: Yeah, Megan. So as many of you know, we've talked briefly that there are quite a few breaches of information occurring not only in health care, but all industries. And whether or not they're effective is actually a question-- several organizations have done research on-- whether that's Carnegie Mellon or several others that have looked at whether or not notification of individuals actually helps.

And from my perspective, I think it does. And I say that for two reasons. One is the organizations that are either attacked because of a hacker breaking, as Andy mentioned, or whether it's an individual has lost a laptop or some variation, you need to be accountable for responding to that breach and notifying individuals that they do have a risk of some form of identity theft.

And as such, essentially instituting not only processes, but policies and technologies that help reduce the risk of that occurring again. So it does put the burden on the organizations that are losing this information, having it stolen from them to take action. So the breach itself is an event that is now causing organizations to take appropriate action.

For the individuals themselves, whether they're seniors or any people of any age, whether children or other ages, receiving a breach notification doesn't necessarily mean your identity has actually been compromised. But it does put you on the alert that the information has been made available in the black market, or at least in some form outside of your control. So that you, as an individual, can take the appropriate steps to protect your identity.

Whether it's getting access to those free credit reports that one of the panelists talked about earlier or whether it's freezing your credit in some form. If you're in a retirement home and don't necessarily need to open new credit lines, it puts the person on notice that they should or could take action if they're concerned about this.

MEGAN COX: And Robin, beyond credit freezes and credit reports, are there other tools that victims can avail themselves of to recover from ID theft or if they do receive a breach notification?

ROBIN SLADE: Yeah. Well, there are very good, very reputable victim assistance and patient advocacy groups that exist and can help the seniors through the process to understand what the steps are. But typically, once it occurs, often the patient whose ID has been stolen is going to need to prove that they're not the individual who received the service.

My suggestions would be first to start by contacting the billing department of the medical facility or the doctor's office. And if they seem unwilling to help, call the attending doctor or call their fraud or legal department if they have one. Ask what proof they have that this is you.

They typically have a physical description of whoever's been in there-- height, weight, sometimes blood type. Sometimes even the sex doesn't match. So those are the things they should look for.

What date was the service provided? Were you home? Were you at a different appointment?

What services were provided? It is it something that you could prove you don't have a scar, so that you couldn't have had that surgery?

What social security number was used? And if it is yours, then you need to take extra steps to obtain your credit report and ensure that there isn't financial-related fraud associated with this as well.

If your insurance information was used, you need to report it to your insurance company and request that a new ID with a new number also be given to you. And you need to file a police report, which we heard earlier in the last panel. That's an important step in the process.

And then, once your provider agrees that they understand that this is fraud, get from them a letter of clearance and keep it in a safe place forever. And make sure you have that so that you can show that you've been a victim of this type of fraud.

MEGAN COX: Thank you.

PAM DIXON: The single most important thing that a victim of medical identity theft can do is to make sure they have a copy of their health care files before the crime happens. Because there's a lovely catch-22 in HIPAA.

And what happens is that if you call up a health care provider and you say my identity was stolen. The record you have, it's my name and my SSN, but it's not me. You have about a 50/50 chance of that health care provider going, oh, OK. End of discussion. And they won't give you the file.

We've had far too many walkthroughs with victims in our offices since 2006 of this case. So I just say it everywhere I possibly can. Everyone, please get your health care files before you need them. And the best way to do this for seniors and for everyone is to when you have a doctor's appointment, at that appointment-- and for seniors, the doctor's appointment may come to them. There's a lot of mobile services in the senior space and it's really important that they have good access to their health care file-- to make a written request or their power of attorney folks make a written request for their files and keep them in a safe place for them.

And that way, if there is a problem, you don't have to have a pin in your right leg that show's somehow that it's not this person. Sometimes the cases are very close. There can be similar blood types and there can be a whole lot of problems that are prevented by just simply having that health care file in advance.

If you don't have the health care file in advance , one of the most effective things for victims to do, including seniors, is to ask for a John and Jane Doe file extraction.

For those of you who are health care providers who are in the audience, you already know what I'm talking about. For the rest, it's too lengthy to describe here other than to say you remove the fraudulent information and cross reference it with a number, so that life-threatening information is no longer in the senior's file.

I explain this in great detail on our medical identity theft tips for health care providers. But I really focus on the health care file because that's where all the harm is. And you really want to fix that first, and it can really take a long time. And you really, really hope for a health care provider that is not involved in the fraud. Because again, here we come back to that evil catch-22.

Under HIPAA, the health care provider is the one who must provide the file. And the health care provider is the one who must correct the file. If the health care provider is the one who's committed the crime, they will not want to increase their liability by giving you a correction to your health care file. So this is a very tough aspect of the crime and I don't want to sugarcoat it and make it seem like it's OK.

So get the file early and watch out for those free services because some of them are really scammy. And really, really watch those EOBs.

MEGAN COX: And as we're talking about health records, Rick and Andy, could you touch upon how the shift to electronic health care records might change privacy rights or what trends that could come about?

RICK KAM: In terms of the move to electronic health records, I think it actually increases the complexity of maintaining privacy rights. Pam mentioned HIPAA, Health Information Portability and Accountability Act. The whole intent of HIPAA was to provide some level of privacy.

However, I think the opposite, the unintended consequence of HIPAA is, as Pam described, to an individual, the inability to actually access your own health record if it's been compromised by an individual-- a bad actor.

But the other aspect of i quite honestly, with electronic health records focuses more on the information and security aspect of this. We haven't really talked about the actual impact on the industry itself. The source of these records is the health care industry and all of the millions of business associates that they work with.

I mentioned earlier, 300,000 covered entities are involved in providing health care in the US. There's somewhat on order of 3 million other organizations that help provide the data infrastructure to support electronic health records in the US. And the combination of these two types of organizations-- one's providing health care and one that's helping manage health care information-- actually creates tremendous information security and information privacy risks.

The good news is there's a lot of benefits to electronic health records and the opportunity to improve health care and the cost of health care. On the other hand, technology and the consolidation of these records creates risk.

And in fact, one of the studies, most recent studies that we did with the Ponemon Institute, looked at how many people are actually impacted on an annual basis with medical identity theft. And what we found was 1.85 million people were falling victim to identity theft in the study

period, which covered the last couple of years. And equated to $41.3 billion in medical identity fraud. So this is a serious problem from a privacy and security perspective as well as a cost perspective that it's occurring in the country.

So electronic health records. Good news is it does help with a lot of aspects of our health care system. On the other hand, it does provide risks that we need to address.

ANDY MCKEE: I would agree with Rick. Again, I think it's a double-edged sword. The same thing that makes it attractive to providers-- it makes everything more efficient, more easily to manage-- also makes it very attractive to criminals. And in our Office of Audit Services, they did a study a couple of years ago. They went out and they looked at seven different hospitals and just looking at them for HIPAA compliance.

Hospitals and providers will tell you, yes, we're compliant. We think we're compliant. So our auditors went in and looked at, again, these seven different hospitals. And they found things such as passwords that were freely shared among administrators. Or they found instances where employees were terminated. But their access to the computer systems usually weren't done. They were done on a two-week rotating period.

So you may have terminated somebody on Monday and their password wasn't cut off until two weeks because that's when all the password were cut off. So you basically had an employee who was very angry because they had gotten fired that has, basically, two weeks where they can access anything within the system. So basic controls like that were just not in place. In a lot of different types of organizations, that's true. But within hospitals and health care organizations, there's an increased risk for that.

And again, with electronic health records, if you go into a hospital these days, you see people walking around with laptops, little carts rolling around. If I was a bad guy, I could probably walk around a hospital with all types of antennas hanging off my laptop and nobody would ever say a word to me because it's what everybody else is doing.

Again, so there are certain records. Again, I think electronic health records cut both ways.

RICK KAM: And just one more comment to just add up to what Andy's talking about. In the survey that we talked about earlier, what we also found was three of five organizations don't dedicate the appropriate resources to protect these electronic health records in the first place. And the executive teams of those organizations don't necessarily recognize the risks that are associated with that data.

And one of the things that we uncovered in working with these organizations, the health care organizations in particular, is that one of the problems we see is that information in general isn't valued. If you think about-- and this came to us, actually, from a meeting we had in San Diego. Pam, you might have been at this meeting.

But what we discovered was the accounting systems that we use today to account for the value of assets was literally designed 150 years ago to value things like buildings and trains and oil wells

and things like that. However, if you look at today's balance sheets, income statements, the tools essentially that corporate entities use to value assets, there's no line item for the value of data.

So what happens is when an organization is unable to value an asset, it makes it very difficult to appropriate scarce resources to protect that asset. So one of the things we uncovered was this basic problem of valuing data, which has become the core of our economy, which is a very serious problem.

MEGAN COX: And do you think HITECH, the Health Information Technology for Economic and Clinical Health Act, will help businesses come to realize that, as state attorney generals can bring enforcement actions and that companies will realize the value of that data and invest in protecting it?

RICK KAM: I do believe that, over time, the enforcement actions that will come under HITECH will help organizations, even though they won't realize it at the time when they're being fined or investigated.

What we're finding is within the organizations, the people that are responsible for privacy, security, and the operation side of the business understand the problem. They understand this information has value. They understand that it's being lost, stolen, and misused. But there's a communication gap that exists between those individuals and the executives that are essentially assigning and aligning resources to protect this in the first place.

They speak different languages. If you imagine going to a CFO and basically saying, we need to implement these-- a new electronic health record system. We also need to make this investment in information security and privacy. The CFO basically is going to ask, so how does this investment compare to, perhaps, implementing or building a new MRI center, or putting in place a new website that might be patient-centric?

And unfortunately, the people that are operating in privacy, security, and even IT don't speak the language of the CFO. They just don't know how to answer that question. So there's been a lot of activity recently, in particular-- again, from the American National Standards Institute, the Internet Security Alliance, and the Sante Fe Group, which Robin is also a part of, to help to create a tool, essentially, that will allow people within your organization to communicate better along the lines of understanding what the risks are associated with this information, what the investments are necessary to secure it.

And more importantly, how to actually communicate on what the risks are. Because it turns out the risks are advancing rapidly with new technology being introduced into the health care industry.

And by the way, that ANSI document is free. It's at ansi.org/phi. So if you go there, you'll find this particular document that describes how to communicate with the CFO.

MEGAN COX: Great. Thank you. So as we are shifting gears to recognizing the risk, to now talking about solutions. So Robin, could you talk about some individual-- what individuals can do to help be a solution to this problem?

ROBIN SLADE: I think we have to start with education and awareness. My feeling is that the lack of education is among the root causes of the proliferation of fraud. And I think if we can do a better job of making individuals understand the issues that are associated, what the red flags are associated with medical identity theft.

I think we also need to find ways for the consumer to play an active role in fraud prevention. And they are the only ones who know whether they've received a service or not. So we need to embrace them in the process.

As far as industry goes, the expanded and increased regulations are going to force organizations to work towards developing policies and procedures that will help ensure that the-- well, hopefully, that the data is better protected.

Rick mentioned that the Ponemon study that ID Experts sponsored-- organizations are saying they don't have enough resources to ensure the data security. But they don't understand what's needed and we need to work towards having a better understanding from the industry level of what they need to do in order to safeguard the health records.

MEGAN COX: Great. Rick, do you have anything to add about industry as part of the solution?

RICK KAM: I think industry, working along with the federal and state agencies, it's important that we value the data in the first place. I think that's one step in appropriating resources to secure information.

I think the other aspect, as Robin said, is education. I think, literally, what we're seeing is a lack of understanding in this whole arena in terms of what the impact to individuals are, to individuals who are seniors or children. There's just a lack of understanding. And so there needs to be research done. There needs to be more people like Pam that are identifying this problem and literally screaming at the rooftops to say this is a specific issue that needs to be addressed.

And then there needs to be incentives provided by the federal and state governments in order for organizations to be focused on solving this problem.

MEGAN COX: That's a nice segue into asking Pam and Andy what they think the roles are for federal and state governments in this.

PAM DIXON: No? No one wants to touch that. OK.

There's a couple things that would really help this. Certainly, a national level set of best practices. I'm going to hesitate to say regulation because we all know what a vortex that is. But surely, health care providers and other stakeholders can come up with a national set of very simple-- I shouldn't even say this, but best practices for victims.

If folks can agree on what to do to prevent the crime, I think we all need to agree on what we can do to help the victims. So today, we're talking about senior victims.

I think that this should be the highest priority. These folks are extremely vulnerable. They're not going to necessarily know. I did just the most harrowing research a couple of months ago in an Alzheimer's care facility and it was appalling because the care with which the patients were treated was just fine. But the records were just really opened and really easy to access. And there was a number of mobile folks coming in and whatnot.

There's best practices we can really take good care of. In mobile care, we're-- for active seniors who are in still active living facilities, for seniors who are ambulatory and living at home, there's a range of seniors we can really help and develop best practices for them.

Certainly, we should be able to help patients correct their health care files. And this should be a very high priority to guard their health.

In terms of federal and state stakeholders, this is a really tough crime. We really appreciate the prosecutions the DOJ has undertaken and the investigations that HHS OIG has undertaken. They have been instrumental in understanding the workings of this crime. Without them, we wouldn't know anything about this. Really, we wouldn't. So I think more of that is really helpful.

ANDY MCKEE: I would think there are certain things that can be done. I know, for example, down in Miami-- obviously, it's a high fraud area-- explanation of benefits used to go out, I believe it was on a quarterly basis. I believe they've upped those up to a monthly basis in some cases, just because it's a little bit quicker turnaround time.

And I think Pam mentioned this earlier, and I don't know-- this is a very difficult problem to solve, but the fact that Medicare numbers are social security numbers. How do you fix that?

Because from Medicare's perspective-- I'm not a Medicare apologist-- but what do you do if somebody's number becomes compromised? You can't say, OK, well, that person is no longer going to get medical services under that number. Because what if the patient turns around and does need those services? What if they do need a wheelchair? What if they do need heart surgery? But hey, somebody's already billed for that.

You can't just say we're not going to pay for that anymore. So I think the government's kind of up against a rock at that point. Again, because you want to make sure the beneficiaries get the services they need. So I don't know what the answer is to that.

I know there have been some test projects where there's been some talk where Medicare beneficiaries maybe get something like a credit card. And those numbers-- like when a credit card becomes compromised, you can cut that credit card off. And their Medicare number would not necessarily be their social security number.

I think that's a really problematic-- again, they've been paying that way for 50, 60 years. I don't know how they're going to do that and how you would do that. Again, I know there's been some

pressure for them to come up with an alternative. But again, I don't work for Medicare, so I don't want to say what they can and cannot do. But again, it's a very difficult problem to fix.

MEGAN COX: Thank you. Well, we want to leave a few minutes for questions. But if we could just go down the line and maybe everybody, in a minute or less, could highlight the one or two things they would want to see happen.

I know changing Medicare numbers and consumer education are a big part. But if you can make one or two things happen in the realm of medical identity theft for seniors, what would they be? Pam, do you want to start?

PAM DIXON: That it never, ever happen again. That would really be what I want. Barring that, I would really like for patients to be able to access their records and have corrected records. In particular, seniors. And without undue fuss because that's a real problem.

MEGAN COX: Thank you.

ANDY MCKEE: I would just mirror kind of what Pam says, that it doesn't happen. Again, I've talked to Medicare beneficiaries who have been the victims of this and it's heartbreaking. Again, a lot of them are victimized are the most vulnerable among us. So just to have it stop completely-- yeah, that would be great.

RICK KAM: I actually wanted to echo something that Pam started earlier talking about. It was no social security numbers on Medicare cards is one thing the federal government can do to reduce the risk to seniors.

The other thing though, we talked about not only in the context of medical identity theft, but other forms of identify theft is monitoring, essentially, your statements. I think Robin, you brought this up.

One thing Medicare could do is actually create readable, simplified electronic explanation of benefit statements, or statements at all.

It turns out, in some states EOBs are not printed for Medicare recipients. So they have no tool actually to-- even if they could read their EOB, to know whether or not a transaction has occurred or not. So one thing the federal government could do is actually not only print or transmit EOBs, but actually make them readable.

I don't know if-- many of us have received health care. If you try to read these explanation of benefits, you start out at the very top saying this is not a bill. So just deciding whether or not to open the mail is one problem. Because you don't want to waste your time on all this if it's not a bill.

But once you do open it, essentially, it goes through line item after line item of transactions. You have no clue who or what actually occurred and what time frame. Then, whether or not you're

supposed to pay for it or who's going to pay for it. So perhaps having an EOB simplification requirement that starts in Medicare might be helpful.

ROBIN SLADE: Well, I would, of course, echo what they are saying about consumers. And clearly, greater awareness of the impact and the seriousness of the issues, not just for consumers but also the health care industry as well that I would like to see that.

I'd like to see organizations supply adequate resources to protect the data. And then, I'd also love to find a way that we could authenticate individuals. That they are who they say they are. But of course, the enrollment issues are always, always difficulty. How do you know that they are when you first put them in the system? And then if you get them in wrong, it's a nightmare. So those would be what I'd like to see.

MEGAN COX: Well, thank you, all. So we'll open up to audience questions. We have two people circulating with mikes. If want to raise your hand, they can come over.

AUDIENCE: Thanks so much. I'm Barbara Dieker. I'm actually within the Department of Health and Human Services, but I'm within the Administration on Aging, which is now the Administration for Community Living. And more of a comment and kind of an add to some of the things that you mentioned that would be good solutions.

One of the programs as the office-- I'm the director of the Office of Elder Rights there. One of my programs that I'm responsible for is a wonderful program called the Senior Medicare Patrol Program. Hopefully some of you have heard of that program and are familiar with it. And the sole purpose of this program is to empower seniors to prevent health care fraud.

We basically-- it's a grantee program. We have 54 grants, one in every state, Guam, Puerto Rico, Virgin Islands, and DC. And the purpose is to go out and recruit seniors to basically be trained in Medicare, Medicaid, and other health care programs, but primarily focused on Medicare. And how seniors then can prevent, identify, and report fraud, scams, ID theft, all the things we're talking about.

So they're thoroughly trained, these senior volunteers. And then they go into their local communities and they educate their peers on the very things that you were talking about-- how to read your Medicare summary notice, how to prevent fraud by hanging up the phone when those telemarketers call, how to protect their personal information, and all the other things you've talked about.

And they go out to senior centers and they go out to health care affairs. And they go everywhere. And they work with providers, too, to educate them. And it's a wonderful program. We have 5,000 senior volunteers across the country right now that are going out and working at the grassroots level to educate their peers and get them excited about how they can help save their Medicare. And many seniors view it that way, saving that money.

And to your point Rick, about redesigning the Medicare summary notice. That has recently been done-- more readable. We were asked, as stakeholders, to help with that process. The Centers for

Medicare and Medicaid Services has redesigned that Medicare summary notice to make it more readable and understandable by seniors. And it's a big, big improvement.

And we thought it was so important because, obviously, that's half of what we're trying to do is tell people, how can you read that Medicare summary notice to identify potential fraud, things that were not billed to you?

We also just-- and I won't monopolize the rest of the time here. But the other thing that we do in addition to outreach and education of seniors is we assist individuals. And again, this is beneficiaries or family members, caregivers, whomever, when they have identified a potential issue. And of course, they don't know right off whether it's fraud, or an error, or whatever. But come back to us and we will assist you in either working it through and figuring out if it's an error or fraud, or getting it into the right hands of the people who can investigate it.

We work hand in glove with the Office of the Inspector General, with CMS and others to make sure it gets into the right slot. So I just wanted to put in a plug for this program. If you're not familiar with it and you want more information, just go to smpresource.org. And that's our website that we have for lots and lots of information. And there's a locator for your SMP in your specific state.

PAM DIXON: That's great.

MEGAN COX: Thank you.

RICK KAM: Great. Thank you.

MEGAN COX: We did get-- oh, sorry.

RICK KAM: I'm just saying I got a wish out of the whole thing. That's great.

MEGAN COX: We did get one question in from our webcast. And it is, what legal rights do victims have to correct their medical records? Is there a medical record credit reporting agency where they can check their medical files, or is the Medical Information Bureau of sorts? Robin or Pam.

PAM DIXON: We have a 22-page answer to this question and a 1-page answer to this question on our website. I strongly recommend that this person look at our medical identity theft FAQ for victims.

A health care provider is going to want a full legal medical record of the patient. And as a result of that desire on the part of the health care provider due to malpractice insurance and all sorts of other things like that, and also to prove quality of care and a lot of other complex regulations that they're subject to, they are going to be quite loathe to delete information from a health care file.

Under HIPAA, including under the new ARRA HITECH editions, patients have the right to request an amendment. This is not sufficient in the case-- and by the way, it doesn't always have

to be given. But in the cases of medical identity theft, that's why I was saying we need some best practice guidelines that are national.

Because right now, the patient will be treated quite differently depending on which health care provider they make that request at. Some health care providers do what's called a John and Jane Doe file extraction. And it's an extremely effective way of allowing the health care provider to retain their full legal medical record and, at the same time, removing all of the fraudulent information from the victim's file.

Barring that, sometimes there are no changes made. Barring that, sometimes there are modest changes made. Sometimes there's just a paragraph added at the end of a 1,000 page file. It depends on the particular case of the victim. So the answer to this question is the rights are limited. There's no credit reporting bureau for this. It would be incredibly challenging to do that because this is protected health information. There's significant privacy and liability issues in combining it.

There is something called the Medical Information Bureau. This is not related to what we're talking about today. That's an entity regulated under the Fair Credit Reporting Act and is actually a quite different beast altogether. And it's quite unrelated. I hope that's helpful.

MEGAN COX: Thank you. Are there are other questions in the audience?

AUDIENCE: Just following up on that, what assistance can medical insurance companies play in correcting records, since all of your providers report to your medical insurance companies?

PAM DIXON: Health insurance companies have been incredibly helpful for all of the victims we send to them. Bizarrely enough, I think it's because their footing the bill. They tend to just, really, be very aggressive with completely correcting the record, completely doing the John and Jane Doe file extraction, changing the billing codes, and really clearing it up.

We've had a lot of very, very positive victim assistance actually from health plans and insurance companies.

RICK KAM: I would add just to-- if you look at health insurance companies, they actually have organizations within their-- departments within their organization that are looking for fraud, waste, and abuse. So it's oftentimes the patients that are finding those particular inaccuracies and calling them and saying, I didn't receive the wheelchair that Andy said he was going to send over, that are identifying this fraud, waste, and abuse.

AUDIENCE: Do you have any information about the doctors who have participated in the fraud, and are they no longer practicing? And how can consumers get that information so they might not go to that doctor or follow-up that way?

RICK KAM: Great Question. I don't know. Do you know?

ANDY MCKEE: I mean, I don't think that I'm aware of any-- well, you could check on a particular physician, usually through the state licensing board. You can find out if there's any type of administrative or any type of action against them. That's probably the best place to go, look at the state licensing board. I think most of those are online at this point.

Again, you can usually just go there and it'll say-- some states are more-- obviously, have better records than others. Some will tell you even if they've had a liability action filed against them as well. So again, I think it's important for the consumers and the patients to be educated and to look. They are consumers at the end of the day, so investigate those providers you have questions about.

MEGAN COX: Any other questions? No? All right.

Well, please join me in thanking our panelists that are here today.

MEGAN COX: And we will now break for lunch. There is a paper in your folders with the agenda and bios of local restaurants if you need some insights on where to eat. And the next panel will convene at 1:30. Thank you

Thank you, all. That was wonderful. That was great. A lot of wonderful insights.