U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Medical Identity Theft Town Hall
October 15, 2008 – 8:30 AM – 4:30 PM
601 New Jersey Avenue, NW, Washington, DC

>>Dr. Robert Kolodner, the National Coordinator for Health Information Technology

I'd l like to thank the Federal Trade Commission for hosting this conference and for the conference center support and expertise that they're providing. And I want to welcome everybody to the town hall and look forward to your active participation because this really is an interactive session and one that we look forward to learning a lot from by your participation. I'm Dr. Rob Kolodner, the National Coordinator for Health Information Technology and I'm responsible for serving as the Secretary's principal advisor on the development, application and use of health IT. My office, the Office of the National Coordinator works across the federal government with health IT programs and provides leadership for the development and implementation of an interoperable nationwide health IT infrastructure. Just so you know, there are almost 500 people who've signed up either to attend or to participate online via the webcast, and we're looking forward to being able to engage as many of you as possible. Participants come from the federal and state governments, from academia, healthcare providers, payers, associations, vendors, the press and private citizens. That perspective of all of those different points of view is important for us to really understand the full scope and depth and sensitivities in this area. As you probably know, health IT is in a central part for vision of health and well being. And in particular of a healthcare system, it puts the needs and the values of patients first, and one that gives patients the information they need to make health-related decisions often, in consultation with dedicated healthcare professionals, but much for health also comes from non-healthcare related aspects. And it's important for that information also to be very personalized to our particular situations. Health IT can be a valuable tool to help us to reduce errors, deliver high-quality healthcare and to provide affordable, efficient healthcare across the nation. ONC is proactively involved in the issue of medical identity theft because it has a direct effect on consumers and patients. Having the wrong information associated with you can be dangerous for your health. Such effects could result in the inclusion of inaccurate information in the individual's health record, having to do with blood type or prescriptions which could then affect decisions that healthcare providers are making on your behalf in terms of your current or future healthcare. It could result in denial of health insurance or other possible misuses of health information for public health and research that would be inaccurate and would--could result in decisions that are not ideal for individuals or for communities.
It can have an effect on the reliability and accuracy and efficiency of the electronic health records which are just now coming into the fore and beginning to be used in this country. And it could limit the advantages of the electronic

records over the paper-based systems if the medical identity theft results in the increased cause or unreliable information. So, the purpose of the project is really to hear from as many stakeholders as possible in terms of the scope and extent of the problem and the speakers to day will be covering a number of areas and eliciting your input. So, we encourage your participation in the town hall and sharing your perspectives and experiences to help us understand and tackle this challenging issue. Our primary focus is the impact on an individual and how health IT can be used to help with prevention, detection and the remediation of medical identity theft. And we seek to have an open dialogue, identify the synergies and foster ongoing cross stakeholder collaboration. And we encourage you not only to share your ideas and suggestions with us today, but even after this town hall, we plan to provide opportunities for you to continue to communicate your ideas and suggestions as we learn more about this emerging issue. With that, let me turn this over to the person who's really been responsible for leading the effort in my office, Jodi Daniel--her biography or bio sketch, I think, is in the packet--but she is the Director of the office of Policy and Research in ONC.   She's played instrumental role in key policy issues within HHS such as the HIPAA privacy rule. It's been a real pleasure to, for me, to be able to work with her since I came over to HHS and I'm pleased that she's now leaving--leading this, wrong word, as a psychiatrist. No, is that she is leading this proactive effort for the issue of medical identity theft. And again, we look forward to a lively interaction throughout the day. Thank you.

>>Jodi Daniel, Director, Office of Policy and Research, Office of the National Coordinator for Health Information Technology.

Thank you, Rob, for those opening remarks and I'm glad that you've been able to take time out of your day to be here as well and good morning everyone. Thank you so much for your interest in this conference and for taking time out of your busy schedules to participate in this event. This is a very important issue and it's very exciting that we have such a great diverse group of stakeholders here, both from the public and private sectors to engage in a dialogue about this issue.
I'd also like to take the opportunity to thank the Federal Trade Commission, and particularly Betsy Broder and her staff who have not only provided us with this meeting space, but have been providing us with ongoing advice as we've begun to study this issue. It's been really invaluable to us. I'd also like to thank the numerous people who have participated in, and contributed to the environmental scan which will be available later today and to our panelist who are here today as well. I'm sure everybody attending the conference today, and hopefully listening on the web soon, has heard about identity theft in general. And actually, by show of hands, at least for the folks in the room, who has been a victim of identity theft or know somebody who's been a victim of identity theft? Wow, so we've got about half of the people in the room raising their hands. Now, who in this room has been a victim of medical identity theft or knows somebody who's been a victim of medical identity theft? And we've only got about five hands or so in the room which is what I would expect. Medical identity theft is a less well-known

form of identity theft and less we'll understood. It's not as well documented. And the implications of medical identity theft may not be known for sometime. So, it's something that we really need to think about who we can best understand, determine the scope of the problem, and how we can figure out how to help consumers to address issues when they have been a victim of medical identity theft. This is something that's a real concern that every American should be aware of. As Rob had mentioned, it can result in the wrong health information getting in your health record, and that can impact your ability to obtain healthcare, your health insurance or life insurance, and most importantly, can impact your ability to get the appropriate medical care and have devastating consequences. That's why ONC decided to take a proactive approach to looking at this issue and to studying this issue. We want to understand how health information technology might impact medical identity theft both positively and negatively. We want to anticipate any pitfalls and make sure that we're taking steps to address them. We also want to take advantage of the potential that health IT might have to both prevent and detect medical identity theft so that we can take advantage of those opportunities as we are building the nationwide health information network considering how we can build the appropriate protections into the technology and into the processes. We also want to look at how other industries have dealt with identity theft and try to take advantage of what they've learned, and the protections they've built into the technology to both minimize identity theft and to protect records. This is just the very beginning of the dialogue. When we first started down this path, we wanted to make sure that we understood what the issues were before we figured out what steps we might take or the private sector might take to address the issues. That's why we're here today. We're going to start by talking in depth about what medical identity theft is, the scope of medical identity theft, and how the people technologies and processes can impact it. And that takes us to today's agenda. This is in your packets. I just wanted to walk through the day quickly. We have four panels with experts on each of the panels; first talking about the scope of the problem, second, talking about the laws, policies and procedures that are currently in place that may impact medical identity theft, the role health IT has to play in medical identity theft. And then at the end, we're going to have a reactor panel which is going to have representatives from each of the three panels that are going to answer questions and talk about the path forward; what are some of the things that we've learned form the day, what are some of the opportunities that we may take advantage of in the future. Just to go through a couple of logistics, the session will not be a series of PowerPoint presentations. This is the last PowerPoint presentation you'll see today because we really wanted to have moderated discussions and get the experts to talk to one another rather than just to explain what it is that they know and they have to contribute. Questions are welcome. We will have an opportunity for questions after each panel. Those questions can be submitted on the cards that you have on your chair. We ask for those people in the room that you include your name and affiliation and either present it to one of the staff people who'll be walking around or put it in the boxes at the back of the room. And we'll also take questions via the webinar. I don't know if the folks are online yet but there will be a way to submit questions on the webinar via the question box located on the right panel of your screen. For those in the room, there are beverages, snacks and lunch available outside. We ask that you contribute your fair share. There are boxes available to collect money for the food, and we will have an environmental scan available at the end of the day. They'll be available in print form in the room. It will also be available on our website for those who are either on the web or who can't stay all day. A couple of other housekeeping notes--bathroom is past the security desk to the left. If you do choose to leave at a break, you will have to go back through security. So, keep your visitor badges and leave a little bit of extra time to get back in. So, what is medical identity theft? We've defined medical identity theft as the misuse of another individual's personally identifiable information such as name, date of birth, Social Security number, or insurance policy number to obtain or bill for medical services or medical goods. There are a couple of points I want to make about this definition. This is not a legal definition. This is a definition that we've developed as a working definition for discussing this issue. Others have used different definitions either in the context of law enforcement or other studies. So, there are different variations on how folks have defined this. What we wanted to include was anything that had an impact on the health record of an individual. So, we've included both consensual and nonconsensual misuses of somebody's identity for these purposes, and let me explain what that means. In a consensual situation, my sister decides that she needs to get a healthcare service and doesn't have insurance to cover that, and I give her my insurance card. She poses as me when she goes to the doctor and gets those services billed to my insurance under my name for the services that she provided. I know about it, but it's still a misuse of my identity to get billed or pay for payment for healthcare services. In a nonconsensual situation, she steals my insurance card and does the same thing, goes and gets services and I know nothing about it. Either case, there could be wrong information that ends up in my medical record. And so, that's why we wanted to make sure we're including both the consensual and nonconsensual situations. I also want to say that we are not looking at identity theft where it's for pure financial purposes so where somebody steals somebody's identity, even if it's from their healthcare record, and is only using that, for instance, to obtain credit, but where there's no impact on the health information that is held for a particular person. We have not included that in our definition. So, you've heard about Rob and I mention prevention, detection and remediation. And I want to just focus on this for one minute because I want to make sure that we're covering all three of these issues. So, prevention is where someone will put measures in place to stop medical identity theft before it occurs. And this is the ideal of where we want to be because it's less expensive in detection and remediation. That being said, it will be impossible to prevent all forms of identity theft or medical identity theft from occurring. And so, we have to look at detection and remediation as well. Detection is recognizing one medical identity theft occurs, and taking steps to address that. We're hoping that we can figure out how technology can facilitate the detection of medical identity theft. And that's one of our goals today. Remediation is about the actions an individual or organization can take to medicate the impact after medical identity theft occurs. This may be difficult and costly, and it's something that we really want to explore to make sure that we're thinking about how consumers can take action in the event of a medical identity theft incident. As the Office of the National Coordinator for health IT, we're focusing on the role of health IT and medical identity theft. And oftentimes, when I say that people think only about the technology, and I want to make sure that folks understand that we're talking about the technology, the people, and the processes. Technology alone cannot address this issue. It's an important component however. But when we're looking at this, we have to look at what the appropriate processes are that we should put in place to prevent, detect and remediate medical identity theft and how the people interact with both the technology and the processes, and the information. So, we're looking at all three of these things and we'd like to explore all of these issues today. You've heard Rob and I talk about this a little bit already, why are we addressing this issue? We are trying to gain a broader understanding of the impact to a patient of inaccurate information being put in their record--both be relied on to provide treatment, possible discrimination and other implications such as financial implications if they, if their health insurance is maxed out, that sort of thing. We also want to really understand where there are some opportunities. The work that we're doing at ONC is still in the early stages, and we want to make sure if there are opportunities to build prevention and detection into health IT activities that we're thinking about that now.   And most importantly, we want to make sure that we're preserving trust. This is both consumer trust and provider trust. We want to make sure that consumers trust that their information is secure, and we want to make sure that providers trust that the information that they're relying on to make medical decisions about a patient is accurate. These are key to our success in making sure that health information is available at the time and place of care that the trust is there for the information to be exchanged appropriately. And I wanted to finally end with what were hoping to get out of this town hall meeting. I mentioned that this is really an early stage, and we're trying to both get--both educate and promote a dialogue about these issues. We really are fortunate to have a multi-stakeholder forum for discussing this issue, and I think that that's really what's the most powerful thing about today. We want to understand the magnitude and impact of medical identity theft, something that isn't very well understood, and we really want to generate ideas for the path forward to create ongoing awareness and to try to strategize about some next steps that the public sector can think about, and other private sector can think about, and how we can partner together. So, that's what we're hoping to accomplish today. It's an ambitious agenda, and we'd like to get started. I'd like to invite the first panel, the ones we're going to be talking about the scope of the problem up to the podium. While they're assembling, I just want to let folks know that everybody who will be speaking today, their bios are in the packets. So I'm just going to ask everybody on the panels to briefly just state their name, their organization, title, just a very brief introduction and then we'll jump right into the questions. We'll start down the other end while Kirk is getting settled. If you could just come down the line and introduce yourself to the audience?

>>Nicole Robinson
I'm a volunteer for the Identity Theft Resource Center and I'm also the victim today.

>>Shanda Brown
My name is Shanda Brown. I'm the Assistant Manager of the HIS Department for Massachusetts General Hospital. One of the primary functions of my, you know, role at Mass. General is to be responsible for the patient index unit which handles any issues of medical identity theft for Mass. General.

>>Pam Dixon
My name is Pam Dixon from the World Privacy Forum. I think most people here know that I wrote the first report, major report on medical identity theft in 2006 and have done a lot of ongoing work about the issue.

>>Lisa Gallagher
My name is Lisa Gallagher, I'm the Senior Director of Privacy and Security for HIMSS. As a background, HIMSS recently conducted a comprehensive security survey and in cooperation with ONC and Booz Allen, we added some questions to the survey regarding healthcare organization's recognition of the problem of medical identity theft. And I'll be providing some of that information as background.

>>Linda Foley
I'm the founder of the Identity Theft Resource Center. We work with victims of identity theft. We also work with victims of identity theft. We also work with all business entities, governmental and agencies looking for solutions and exploring the problem of identity theft of all aspects including medical identity theft.

>>Betsy Broder
I'm from the Federal Trade Commission's, Division of Privacy and Identity Protection.

>>Kirk Ogrosky
I'm from the United States Department of Justice Criminal Division, Fraud Section, and I coordinate in healthcare fraud prosecutions.

>>Jodi Daniel
Great, thank you so much. I'd like to start with Betsy and then Kirk once you get settled. If you could talk a little bit about the nature of the situations that you've experienced or the types of complaints that you've received related to medical identity theft.

>>Betsy Broder
Thank you, Jodi We have two perspectives, at least two perspectives, on the prevalence and impact of medical identity theft here at the FTC. First of all, we do surveys. We think it's important to get a sense of what the environment is, how prevalent these problems are. So, in 2006, we conducted a survey asking consumers what they had experienced in the last five years with respect to identity theft. What we found overall was that there were slightly more than eight million consumers who reported that they had been victims of some sort of identity theft. Four percent of the--I'm sorry--three percent of them said that someone used their medical insurance to obtain care. Another three percent said that medical care was obtained in their name, not necessarily through their insurance, but through some other--they just sort of walked in and it was billed to them. I think that's probably slightly more prevalent. And then, slightly less than half of one percent of all of the victims said that someone was actually able to open up a new health insurance account in their name. Now, this is asking consumers what they know of, what they've experienced in the last five years. We're also aware based upon some of the complaints that it may take quite sometime for people to appreciate that someone else has used their information to obtain medical care. So, we look at this from a survey perspective, but the FTC also has a complaint database. Every week, we're contacted by between 15 and 20,000 consumers on the issue of identity theft. Not all of them are victims. Some of them are just seeking more information, but many of them are. So, in an average year, we may get as many as a quarter of a million complaints from victims of identity theft. And generally speaking, these are people who have the most intractable problems. They're contacting the FTC because they need guidance in how to resolve the issues that they are confronting. So, people who are able to resolve them themselves, they may also complain to us but we generally get the more complex cases. So, we went into the database to look at what types of complaints we're getting from victims of identity theft. Now, these may not be typical, as I said, these maybe the more dramatic ones but I thought that it would be helpful. We'll hear also from the Nicole who we worked with closely over since we started our identity theft program, really, on her perspective; but these are some examples. One says I first noticed the account when I was trying to refinance my home. I notice that there was a medical collection on my credit report. Skipping down, she said, "There actually were children who were getting medical care using this person's information." There are three different children getting medical care. The impact on this consumer was credit-related--that at least as far as she knew it, she was not able to refinance her house because of the delinquent credit associated with the care for the children. The question that probably she would have to pursue after she discover this is to look at her children's health records to determine that there was no corruption of that information. Someone else reported that his house was broken into and his birth certificate, his medical insurance card and his ID were stolen. He pulled his credit report and he found a hospital bill for almost $30,000.

He contacted the hospital to try to resolve this. They told him--he said, “How can I resolve this?” And they said, “Actually, quite easily, just pay the bill.”
And then the question, of course, that needs to be asked of this consumer is look at your heath records. You know, have you looked at your, either your explanation of benefits or some other records that may not be reflected on your health insurance explanation of benefits because there may indeed be some corruption. And of course, as Jodi and Dr. Kolodner pointed out, people may not find this out, that there’s a corruption of their health records until maybe a pivotal and critical point in the delivery of care. I could go on. I mean there are many of them. The only other point that I would make. And again, I want to stress, this is not necessarily the statistical norm because these are based upon self-reported complaints. But it just so happens that in a series of complaints that I was reading through, there’s a common feature. My ex-wife since 1998. My brother has used my Social Security number, in reference to your sister. The people I was living with used my information. My brother used my name, date of birth and education. And I think we will hear from the department of justice, you know the extent to which this may be one of types of uses of medical care when the care is needed and to what extent it feeds into the billing situation and is done solely for financial gain.

>>Jodi Daniel
Do you want to follow up on that?

>>Kirk Ogrosky
Sure. There’s--from my perspective, and let me back up a little bit and tell you a little bit about the Criminal Division and what we do. We’re not typically, when you hear about healthcare fraud and abuse, the abuse part is really not what the criminal division is spending its resources on. We’re talking about the outright frauds, stealing from our government programs and private insurance company. So, we’re out on the margin dealing with criminals who are looking for ways to take advantage of weaknesses in the system. And what we see across our cases is that in areas where there are low barriers to entry, meaning your Part B Medicare providers such as DMEs and other kinds of providers, we see that there’s an extensive use of stolen physician information and stolen patient information. And what we see in our cases largely is two fold. And I’ll give you some case examples and I’ll talk about it; but I want to make sure that you understand that we’re really talking you about cases out on the margin where people are intending from the very outset to defraud our programs. So, the first thing I can talk about is the ease with which people are stealing patient information. And within the last couple of years, we’ve seen some pretty big cases where a low level employees and medical clinics or doctor’s offices--we use a thumb drive or disk to download patient information. And there’s actually a marking on the street in certain communities, particularly in Miami-Dade County where if are out on the street with a thumb drive with patient information, you can actually sell it and the going rate’s about $25 to 50 a name. And part of the problem that we see there is the basic information that’s necessary to file a claim

on our program is pretty simple. If you have a street address, Social Security number which is also the Medicare number, and a name, that's generally enough to file a claim that's going to get paid through Medicare Part B. So, we're not talking about downloading all of the patient's information. We're not talking about medical history. We're simply talking about people stealing the Medicare number, stealing the name and the address. On the physician side, we see the old UPNs tend to be circulated throughout the community that's committing fraud. So, most of the doctors that we have in our criminal cases are complicit. But what happens is, we have a way that we argue this to jury is in for the penny and for the pound. And what we see is the physicians that get involved in these things, whether it's selling prescriptions in part, for Part B services or getting involved with a corrupt clinic, what happens is they're in, they're working at a clinic or they're involved in a fraud and they might decide to get out or go do something else. But once those people that are stealing money have that information, have the doctor's name and the UPN or now the MPI, they continue running those numbers and submitting claims. Let me talk about a couple of cases very briefly that I think illustrate the point; there's two fairly large cases that we're seeing; one involving the Cleveland clinic down in Naples, Florida, the other involving a series of DME companies--cases called "All Med." Both involve substantial billing, and both involve very narrow periods of time. One of the things that we notice in our criminal cases, and if you look across all of the criminal cases brought by all of our U.S. attorney's offices and our prosecutors here in Washington, the cases where we see stolen patient information and stolen physician information typically are short-term, hard-hitting frauds meaning 90 to 120 days. And when we talk to cooperating criminals, what they tell us is, if we do it within 90 to 120 days, by the time people start calling the hotlines, we're gone. So, we can steal the information, we'll submit millions of dollars in claims and then we'll disappear. And they're typically is what we call "nominee owners" to put the businesses and names of individuals that are not particularly interested in healthcare, don't have any experience in healthcare. The All-Med case began back in 2003 with about 50 different DMA companies using a billing company, and All-Med was a billing company ran by two individuals that have entered guilty pleas down in the southern district to Florida, again in Miami. And all of these companies were in Miami. What we found in All-Med was all of the DMEs, about 45 to 50 of them, were submitting claims for prosthetic limbs and orthotics that were very expensive items, custom-formed fitted orthotics. And what we saw was that groups of patients tended to have something in common, and we didn't quite know what that was. And as we went through the cases, what we found is that there was a link back to a cardiac clinic. And what we ultimately learned was that a young lady who had been working on that clinic simply took a thumb drive, plugged it into the office computer and downloaded all of these names which were then circulated. Now, if you go through the case and you look at how it played out, each of the DME companies that were billing for the orthotics and the prosthetics were building for patients that absolutely had no need for any of this equipment. And this case has actually been fairly, widely reported, but one of the interesting things about the case, was they actually stole the identity of the former chief judge, the federal district judge in the southern district to Florida. His name is Edward Davis. And he testified on behalf of the government that he didn't really need two prosthetic legs because he had his legs. In addition, the total billing coming out of these DME companies was around--I think it was $400 million dollars and Medicare paid over a hundred million dollars. And each of the DME has only submitted claims within that 90 to a 120-day window.

>>Jodi Daniel
I may try to move this along because I want to make sure we have an opportunity to hear from all of our panelists and to get some discussion going. Shanda, can you talk a little bit about some of the cases that you've heard and also some of the implications from a provider perspective and also from a patient perspective that you've seen?

>>Shanda Brown
Sure. We at Mass. General over the past 18 months have had about 33 issues we've confirmed as ID theft, and those range from sort of what that scene Kirk was talking about where we contacted the patient's wife because the patient had supposedly presented to the ED and the wife kind of stated, "That's funny because he's sleeping in the bed beside me." It turns out that the patient's brother had present in the ED claiming to be the patient. We have had victims who have three brothers we had at one point in time who were using the same name for immigration purposes. They were all sharing the same medical identity at the facility. We finally had reached a point where we've gotten two of them in the same room together and realized they're using the same ID and had to break that apart. We had a patient who was admitted and we contacted the next of kin that stated the patient couldn't be in the hospital because the patient was incarcerated. We came to find out--our investigation found out the two patients had been incarcerated together. And upon release, one of them had taken the identity of the one that was still in jail to get medical care. So, what we have found from our investigation is that the large majority of these are sort of when in the office, we're, you know, explaining to them, or we'd mentioned where these are people that know the patient and are using information with our without their consent. In terms of impact, we've had several patients who came in where they've had a family member use or a friend or someone that they think they know, using information without their consent and, you know, that does have an impact. We've had, you know, again, the brothers or another case where we've had to explain to them how this has an effect on them clinically, and we are not an investigatory force. We are here for healthcare. We are here to help.
And clinically, it's just a very bad idea to have three people sharing the same medical identity in a facility.

>>Jodi Daniel
In terms of potential for patient care, I think Nicole's probably the best person to talk about that issue. Nicole Robinson, can you talk about your experience and the implications on you?

>>Nicole Robinson
I could certainly sit here and talk all morning. But, since I have a really short period of time, I'll tell you what I know. I know that a woman named Nicole Robinson worked at a place called Caremark which is a pharmaceutical company, and she stole my identifying information. With that identifying information, she opened credit accounts. But because of her use of my information, I have started to receive collection notices from doctor's offices.
I even had an emergency room doctor's bill placed on my credit reports.
I've also received her dentist's bill at my home in Maryland. This woman lives in San Antonio. I know that she is in very poor health. I know that she has a website up currently where she's soliciting donations for gastric bypass surgery, and I know that her use of my information has caused me to get medical bill sent to me at my house in Maryland. What I don't know is that she is constantly doing this. I don't know if she's walked into a hospital and presented herself as me. Because of privacy rules, I can't know that. And that's the part that scares me the most. I know this woman is ill. I know that she has a condition that could cost me dearly and more than just financial ways. And that's the part about her using my identity that scares me today.

>>Jodi Daniel
Pam, do you have anything to add to this as far as the types of cases or the implications? I knew you've been looking at this issue for longer than anyone else. And what can you tell us about it?

>>Pam Dixon
I think there are a lot of issues here. I think the first thing I'd start with is a structural issue. When you compare what Shanda has said and what the DOJ has said, it's immediately apparent that we're really seeing two operational structures here. There's an insider crime where it's more to a large scale, more systemic, and much more difficult to both detect and to eradicate.
And then there's what I call one-offs. What we have really seen in this particular crime and the way it operates is that most of the time, it's only the very worst cases in terms of the systemic cases that are discovered.

>>Jodi Daniel
And I'd actually be interested to hear more from you about that but it really seems like the worst of the bad apples fall off the tree and make a little, enough of a noise that someone notices.

>>Pam Dixon
But the one-offs are more simple to detect for a lot of reasons. And then, of course, there's the clinic takeover operation which I would include in much more of a systemic thing. So, I really do think that you have to consider both structures.

>>Jodi Daniel
Which structure causes the most harm?

>>Pam Dixon
The answer is they both do. Anytime, there's a change to the healthcare record, you've got a problem. And you've got a problem for public health, and you've got a problem for individual care. In terms of what happens to the victims, I mean one of the reasons that I wrote that report in 2006--actually, it started in 2005 with testimony to the NCVHS--the reason that I started focusing on this was because the crime existed but no one was really looking out what was happening to individual victims. And what we were seeing is that individual victims were saying, you know, "This has happened, I went to the hospital and they refused to give me a copy of my healthcare file." We get calls like that every week.
"I'm a victim of medical identity theft," and we can kind of tell what the thing is going to be. "I can't get a copy of my healthcare file." Then they'll call up three weeks later and say, "They won't change it." And then you start the real long process of, "Well, okay, let's kind of, you know, walk through this landmine."
But that's the scenario. I'm very, I'm very reluctant to say that there's an easy fix in health IT. I do understand your focus on health IT as a detection mechanism and as a potential preventive, but I have to tell you, I think from what we've seen, I mean we have a victim from Long Beach for example, and this victim had no idea that her healthcare information had been spread to multiple providers through the pilot project. And unless she had called us, she would never have known. So, I think that health IT, unless there is something very specific done to mitigate healthcare fraud within the system, I think that healthcare IT can actually be an engine for medical identity theft. It can also be a help. So, it thinks that it's good that we're having this discussion today. But I would just caution and say that since 2006, since the report came out, one thing that we're troubled by is some of the mitigation strategies that have been put in place, and one of them is what I recall TSA style authentication in hospitals. You know, we were approached by a vendor who really thought it was a fabulous idea for a palm vein scan to prevent medical identity theft. And actually, there are a number of hospitals how where if you check in, not on the emergency side but more on the, you know, more elective side, you give a palm vein scan. And this is to tie it to your identity and then, you know, prevent medical identity theft. Well, this is fabulous for preventing one-offs that, the one-offs that Shanda described.
It does absolutely nothing for the more systemic type of problem. In fact, it's a fantastic treasure trove for the folks who would steal identities because now you get some nice biometrics to steal, too. And one of the things that we're looking at right now is what on earth do victims do when your biometric including your generic data is tied to a false identity? And actually, it's a very thorny problem, and it's quite difficult to resolve. So, I don't think that there are any quick, easy fixes here. I think that the fix needs to be multi agency. I think that the Federal Trade Commission needs to be robustly involved in any fix as well as HHS.

Not to rattle on, my last point.

>>Jodi Daniel
Sure.

>>Pam Dixon
Is that one of the things that we saw in 2006 was that victims of this crime fall just straight between the gaps between HIPAA and the Fair Credit Reporting Act. And what we find--and Linda, you may want to address this as well, what we find is that victims who come to us, and they can resolve and cure if you will the financial side of things much more readily than they can the healthcare side of things. And what we have discovered is that victims tend to give up. I don't know if you have?

>>Linda Foley
That's true.

>>Pam Dixon
But I hope you haven't.

>>Linda Foley
I would never give up at all.

>>Pam Dixon
Good; but we really do find that victims give up. We worked with the victim who had a very serious case of medical identity theft and she was on a surgical table and goes, "Oh, by the way," and it was really important that she did this because there was inaccurate healthcare information. And her medical file was just like, oh, you know. So, we're very entrusted in finding ways of assisting victims in that second leg where it's just so profoundly difficult because healthcare providers can be victims too. And yet, there can also be individual victims. So, we have to look at the entire chain here in the healthcare system, and I think that's a very important and difficult consideration. Thank you.

>>Jodi Daniel
Linda, can you respond to some of those issues that Pam brought up?

>>Linda Foley
Yeah. Thank you. We obviously have at least two sets of victims in this crime, not just the person whose identity has been stolen, but the health providers pouring out services and money as well. So, I'm assuming that most of the people in this room are also victims of this crime because you have lost money or you have organizations within your groups that know that they have lost money because they're never going to recoup that money. We were talking about cases and it came to mind one thing we have not talked about very briefly is the Medicare problem. What we're seeing a lot of is not the one-on-one which is familial; but

rather elderly, terminally ill people who are in hospice where their information is right there. There is a special investigations agent for Blue Cross, Blue Shield of California who has said, “Up to 50 people may touch one patient’s medical records on the way to an insurance claim.” I was at an IBM-GIO conference and our senior IT person said, “A 150 people may see a file and the information on it during a three-day hospitalization.” When you start thinking about it, everything from admissions, to labs, radiology, hospital supplies, how many people in the nurse’s stations, dietary and everything else, that number grows exponentially. Breaches are another area where we are having problems; though I will admit that within-the-health-industry breeches are fairly low, and I think it’s because it’s so highly regulated, but we’re still seeing a large quantity, and the largest probably far is in the area of paper breeches where providers are just simply throwing medical records in the dumpsters behind their buildings. You’re sitting there laughing. You know what I’m talking about. And those records are difficult. One man had throat cancer. He was dying and his identity had been seen while he was in a hospital. And his last wish was, “I want my good name cleared before I die.” And his daughter and I worked frantically to get it done, and we did. He died a week and a half later. That it had led more to his rapid death, I don’t know, but we definitely know that there is stress involved in trying to clear identity theft especially when a person is not allowed to see medical records which is the information if--and I am a victim of identity theft. When I needed to see my credit and the application and transaction records of that credit information, I was able to see it, and we have the Fair Credit Reporting Act and the Fact Act that helps with that. But when we go to medical records, “May I see what services; we’re trying to know,” there’s a privacy issue. So, we need to find a solution. I don’t know what that solution but it’s not through CRA. We’ve got to figure out where that solution lies. We talked about explanation of benefits. I’m a Kaiser member. I don’t get an explanation of benefits. So, I wouldn’t know if some else was using it somewhere in the Kaiser system. How do I know that there’s not a mixed file? We also have people who are demanding to see that misinformation taken off the record when you say, “Well, it will be marked as--this may belong to a second person,” these people get inflamed over the telephone because as the doctor quickly goes through it, they may not see that. They wouldn’t go to file 12345A and cross reference to the original file they want out of the file. They don’t want the imposter in their life, and I understand that because I don’t want that imposter in my life anymore either.

>>Jodi Daniel

A couple of things have come up about the different types of problems, the different types of scenarios for medical identity theft. And Lisa, you had mentioned the study that you had done about. Theft and/or where you’ve had some questions on medical identity theft, and I thought it would be helpful if you could talk about some of your findings from that study.

>>Lisa Gallagher
>> Sure. Okay. HIMSS did a comprehensive security survey so we were talking to technical folks in the organization such as CIOs, CTOs, the Chief Security Officer, the Chief Privacy Officer, the COO and CFO, for obvious reasons, and also IT staff and security staff. In the survey, we included four questions on medical identity theft and I want to note that we used the same definition that ONC has used here for the study that they're doing. The first question we asked was on a scale of one to seven, how would you rate the threat of medical identity theft at your organization? Now, keep in mind, this is provider so hospitals of all sizes as well as physician practices. So, on a scale of one to seven, the average rating was 3.66. So, here we see that there may be, generally, a pretty low or, you know, to medium awareness of the threat of medical identity theft. The second question, "Has your organization considered evaluating and addressing the risk and impact of medical identity theft as part of your overall privacy and security policies?" The percent, in answering the question, and we use the word considered, have you considered including this, was 67.1%. So, we know that from this, that with regard to the folks that are focused on the security and privacy programs within their organization, they do have some awareness and have future plans to include evaluation of the risk here. The third question, "Have you had at least one case of medical identity theft in your organization?" The percentage answering the question, yes, was 20%. We then proceeded to ask the organization, assuming that they had some level of awareness of medical identity theft, "Have you changed your business practices associated with the risk of identity theft, medical identity theft?" And we offered them a number of options, of ways that we--to sort of help them along. The first was has improved patient authentication methods. The number of respondents saying yes, 52.9%. Has a plan in place to report suspected medical identity theft or other fraudulent activities to law enforcement or regulatory agencies, 43.9%. Provides patients with a simplified EOB, 43.2%. Provides patient with clear notice of consequences of sharing health data coverage for purposes of committing healthcare fraud, in other words, do they pro-actively warn patients not to share their health coverage data, 32.2%. Do they provide patients with the resources to identify and report suspected medical identity theft or other fraudulent activities to the organization's management, 25%. So, a little bit lower than the general awareness is the actual process for someone to report a problem.
Aids patient in correcting records that have been corrupted by medical identity theft, 20.6%. And finally, the number of organizations that have not changed their business practices at all in association with this risk is 16.1%.
A full 21.9% don't know what their organization has done to address this issue.

>>Jodi Daniel
So, were you surprised by these findings or was this consistent with what you were expecting to hear from folks?

>>Lisa Gallagher
Well, given the fact that this survey was targeted at IT practitioners and IT decision makers especially around privacy and security, I did expect there to be some level of awareness of this issue. I think that when it comes to connecting the risk that a security or a privacy person might see with a corresponding change in the business practices to enable prevention and detection, I think, we still have quite a ways to go. So, you know, the general organizational awareness, I also think that, you know, monitoring of employee practices and things like that--so the solutions for detection and prevention have not really been institutionalized.

>>Jodi Daniel
Linda and Pam, would you like to respond?

>>Pam Dixon
Yeah. You know, it's interesting, Lisa. I'm sitting here listening to that because we've been watching the studies on the business entities, government and such, those numbers, surprisingly--other than in the financial arena, but when we're talking about credit issuers and so, those numbers are larger and better than we see with credit issuers. So, obviously, the health industry, as a whole, is doing a better job of authenticating, putting procedures in place than a lot of the creditors, issuers in businesses are. So as dismayed as I am to hear that, you know, it's still better than what we're seeing generally.

>>Lisa Gallagher
Thank you. Those numbers don't surprise me at all. They are completely in line with our research and the numbers that we found. We found an extraordinary focus on patient authentication, but not on employee monitoring, and also, almost no focus on assisting victims get through cleaning up files. One of the problems that victims often have, we haven't really talked about this yet is in the more systemic cases of medical identity theft, it's not unusual at all to find a victim who has multiple accounts in multiple states. We have found some victims who have an access to 50 different healthcare providers they need to go to and clean up their bills. And usually, those 50 healthcare providers are in multiple states strung across the country from--basically, you can track it to the Medicare, Medicaid payment system and those little silos that operates out of. It's basically how that's working. It doesn't take long to figure it out and see the pattern there; but when these victims approach healthcare providers, what happens is that, you know, they're coming in cold, they're getting entirely new information created in these healthcare providers and it's quite difficult to authenticate your way out of that situation. It can't be done.

>>Pam Dixon
So, I think that authentication number is a little bit troubling. But something else that's very different about these numbers than the financial sector numbers is if you look at the financial sector, the credit issuers have been just really bad about

this. But there are other sectors or segments of the financial sector that have been actually quite good about this and quite a bit better than, I think, the healthcare sector. And here's how it's different. When you really look at how all of the--more financial forms of identity theft have been mitigated, it's been done differently. It's been done with much more focus on the individual victim. And as a result, the authentication procedures are quite different. Obviously, they are far more regulated under Patriot 1 and 2 and the GLBA, etcetera, etcetera, but there's still a slightly different focus and it's palpable when you start looking at the different systems. When you get into the healthcare system, basically, you have authentication without regulation and it's incredibly problematic. And we have been sounding this alarm for a couple of years. Authentication without regulation is a problem because you've got original information of patients being scanned and added to a healthcare file and this really changes things for an insider systemic version of the crime. It gives the criminal access to much more robust information. In the financial sector, this information is typically kept separate and has different accounting systems. In the healthcare system, we're not seeing that. So, I do think that there are some lessons still to be learned from the financial sector.

>>Jodi Daniel
Great. Are there any other comments that folks have other types of issues that folks want to raise about the scope of the problem? I want to encourage folks, both on the web--I know we finally have our audio up-- feel free to submit questions on the web. There is a box for questions. And for folks in the audience, you have cards on your chair, you can submit questions. There is a box in the back of the room and also some staff walking around who can collect those questions. Linda, please go ahead.

>> Linda Foley
Yeah. You know, in dealing with victims of identity theft, the one thing they want is, they want a clean record. I don't have an answer for victims of medical identity theft as far as how do I clean up a mixed medical file, how do I find out, as Nicole was saying, are those medical--are the collection agencies coming after her because there's a mixed credit file because what you haven't heard is there's at least 10 people using her identity and this has been over a period of, what, nine years now? Almost nine years, yeah. So, is it because they found her name on the credit report or is it because there is a legitimate medical record, and because of private confidentiality, which I do appreciate as a patient, we have a problem in terms of how do I clean up and make sure that that record is not mixed? I'm not going to go to the point where this is life-threatening and I'm going to get the wrong blood transfusion, but I don't want to have my information mixed with anyone else's. My medical history is complicated enough as it is. I don't have a solution for that. I know it's not through FCRA. I think we need to start looking at where can we treat, where can HIPAA help us, where can other entities help in working with the solution so it's not just merge and reading, saying this may belong to a second person; and better recordkeeping to

authenticate each person that comes in. I know that some doctors are taking photographs of patients now which the privacy people are going to go, “Oh, my goodness.” But you know what? As a victim of identity theft, please take my photo. Put down any distinguishing marks. Clearly, I’m going to get older. I’m 6-foot tall--though that’s not going to change too much. My age is going to get older. It’s not going to get younger. There are certain distinguishing things about me that I’m not going to be a 32-year old who’s 5’4 and 101 pounds. I don’t think I was born 101 pounds. There’s got to be a way of marking it carefully so that we can see this belongs to patient A, this belongs to patient B.

>>Betsy Broder
If I may Jodi?

>>Jodi Daniel
Please go ahead, Betsy.

>>Betsy Broder
I just wanted to add one more thing because we’re talking in this panel trying to set up the issue.

>>Jodi Daniel
Right.

>>Betsy Broder
And talking about the scope of the problem, and it’s difficult even with all of the good work that Pam Dixon has done and various surveys that are out there, we don’t know what we don’t know. And if we’re victims of medical identity theft, what you don’t know might kill you, you know, quite literally. So, with--when we look at other forms of identity theft, we tend to evaluate them based upon the financial impact either on the industry or on the consumer, how much money was obtained? But here, even though the percentage of people who may experience medical identity theft is much smaller than other types of identity theft, the impact of that. Can be so devastating.   And so, even though the numbers are smaller than those at large, because of this disproportionate impact on someone’s health and their well-being, their access to medical care at the time that may be critical to them, I think it takes on even greater significance than what the numbers might represent if we look at this solely from a statistical perspective of, you know, what does the pie chart look like.

>>Jodi Daniel
So, we have a couple of questions coming in. And there’s one that actually goes somewhat to the point that you were just making. The question is, what can we do to get better numbers, addressing the scope, and extent of medical identity theft, and then, I guess, to follow on to what you were just saying, Betsy, how can we try to measure the scope of this problem given the complexity that you just raised?

>>Betsy Broder

I think we can--how can we get better numbers? We can try to get better numbers. I think, there just hasn't been a kind of systematic, scientific-based survey. And even if we were to do such a survey, and Pam, you may have some thoughts on this, or Lisa--we have one complaint that I pulled from the database. Someone's information was used for billing when they were 14 years old. And they didn't realize that until they became 18 and applied for credit and they saw all of this medical billing on their credit reports and delinquent accounts. And so, people just don't even know, you know, when it may be happening to them so--but one can only do the best that they can with the instruments that you have and I think that this might be a rich area for greater research and survey work. We, at the FTC, are working with the Department of Justice's Office of Bureau of Justice Statistics. They do a national crime victim survey and they're going to be doing a component on identity theft. It will be the first time that they're doing this in the coming year and that's one way that we can probe these issues.

>>Jodi Daniel

I'm just going to add one more question and then I'll let you jump in. One of the issues in trying to identify the scope of the problems is to identify when medical theft identity occurs. And a couple of people have mentioned how challenging that is. So, as you're talking about this, if you can address that as well. Lisa, and then Linda, and then Pam.

>>Lisa Gallagher

Specifically, with regard to medical identity theft that happens as a result of inappropriate or unauthorized access to electronic health information, what I've noticed in healthcare provider organizations is that there may be a detection of a security breach or inappropriate access but there's not, in the end, a connection made to the motivator, the threat motivator for the breach or the inappropriate access, you know. So, the loop is not, you know--so, until, you know, much, much later when they start to get reports from the patient, that, you know, that will seem to be the trend. And so, one of the things we need within healthcare organizations is to focus on, you know, an awareness that this is a threat.

And also, a completion of the risk analysis cycle so that they go back and take a look at what was the origin of the threat, how was the threat agent motivated and, you know, start to think about that as they do their response to the breach.

>>Jodi Daniel

Linda?

>>Linda Foley

I think we also have to realize that health providers are one of the victims here too and that once they've done their due diligence and they've separated those who just don't want to pay their bill from those who have never had services, you are going to be our greatest measure of how much fraud loss we are looking at.

Kurt, you were mentioning during our conference call about Medicare fraud loss and the numbers just blew me away. There is where our numbers--a lot are going to come from when we separate those who don't pay their bills versus those that is due to fraud, and then it's going to come from the health providers.

>>Jodi Daniel
Pam?

>>Pam Dixon
Thank you. A couple of things--the question that came in were, you know, how can we get more numbers? I can tell you that triangulating these numbers is highly difficult but this is not a new problem. Malcolm Sparrow, for those of you who know him, the Harvard professor has done just an extraordinary and quite definitive work on really trying to quantify healthcare fraud and how it operates. He wrote quite a good book, Licensed to Steal, and I'd really recommend it in terms of looking at the numbers and the scope of this problem. I talked with him in 2006 at length about this and, basically, his idea was that medical identity theft is a subset of healthcare fraud and I agree with that idea. I think it is a subset of healthcare fraud. So, while medical identity theft is a unique and distinct issue because of the specific harm it creates to victims through alterations made in the healthcare file and healthcare records and also billing records, it is still healthcare fraud. And I think, you know, if you look at the scope of this, you really, you have to go back into the food chain of the healthcare system. I think that's where the numbers are, but I still would just assert again that we're really looking at two different types of crimes. We're looking at a one-off crime but we're also looking at a much deeper, more systemic crime and that's the more difficult one to detect, that's the more difficult one to cure but I think that's where most of our impacts are. You can have a person who--all their medical characteristics remain the same--have complete authentication in place, but if someone pops a thumb drive in and does an Isis Machado at the Cleveland Clinic situation, you've got a big problem on your hands to detect, and it's not easy. Malcolm Sparrow's work, I think, speaks well to this. But in terms of risk analysis and your comment about connecting it, I think you're just completely dead on target with that.
I think risk analysis that includes a number of threat scenarios for identity theft financial forms and also medical forms is absolutely crucial and looking at more systemic things. And I just don't think we've looked there yet.

>>Jodi Daniel
I think this is something that maybe we can address later in the day because it's certainly--one of our staff members participate in the phone call, a web seminar on the Red Flag's rule. And we don't need to get into that now but part of that is a developed--what she heard from one of the participants, one of the speakers who is the Chief Privacy Officer for a hospital system in North Dakota, she said, "We've already done this. I don't care whether they're Red Flag obligations or not, this is good practice for us to do." And she created fraud identification, detection and remediation programs throughout the hospital and in networks that

those links were connected. And so, maybe that's something that later in the day we can circle back to.

>>Jodi Daniel
Can you just briefly mention the Red Flag regulations, what they are and who they apply to?

>> Betsy Broder
Sure. Just very briefly, I'm speaking in shorthand so I apologize for that.
There were amendments to the Fair Credit Reporting Act that imposed obligations on financial institutions and creditors who have consumer accounts to have what's called a Red Flags Program. And this is, in essence, an identity theft prevention program to acquire these entities, either creditors or financial institutions to have a program in place that allows them to identify, detect and respond to the Red Flags of identity theft. And so, they would evaluate their particular business, their particular operation to find out how identity theft presents itself, how it most commonly manifests itself and then have a program in place to--when those instances arise, to respond to them, and deal with it both on a consumer and a systemic way to reduce the incidence of identity theft.
It basically shuts down. It's not data security. It's operational, in how you open and access accounts for consumers.

>>Jodi Daniel
Yeah, I wanted to just to add in, the question was, how do we get better data? And I wanted to start with, how we quantify the amount of fraud, and there's a lot of numbers out there about how we quantify the amount of fraud.

>>Kirk Ogrosky
And what I've said before, from the Department of Justice perspective looking at our healthcare cases is we know that when criminals intend to steal from vulnerable programs, if they're doing it intelligently and they're very calculated, they're probably not going to get detected. So, it's hard to put a number on something that's not detected. If it looks legitimate and the claims are being paid and we're not getting reports, how do we put a number on that? That's part of the problem in white-collar crime and in fraud schemes is we know that technological advance helps criminals commit crime. What we have to do in government is figure out how to use that same technology to stay at least equal to or if not, get ahead of them. One of the things that I see in many of our cases is we'll talk to people and they'll say, "Hey, my credit card company can call me and ask me if I'm buying electronics equipment downtown to the tune of $10,000. Why can't my insurance company or Medicare call me and ask if I'm getting a lobotomy? So, these logarithms that the credit card companies have used can be very important tools in detecting and alerting us in the system. We have to advance our identification technology within government, particularly within Medicare. And we have to focus it on areas that we know have systemic, high-crime problems like Part B. In terms of the two types of cases, we really see this

type of theft that we've talked about that has tremendous psychological and financial harm for the individual. We can't prosecute our way out of that problem. We don't have enough prosecutors. We don't have enough FBI agents.
We don't have enough state police and regulators to go out there and try to round up all these people and throw them in jail. And I don't know that that would do a whole lot of good. We try to focus our resources on these large scale frauds to make sure that we're taking appropriate action. But as we can hear and from our--the people that we're talking to and our cooperators, it really is, it's the theft of the future. It's the theft that keeps on thieving, if you will. And what we see is a real problem. And I just want to end with this because we do see patients that talk to us about the real problem. We had a patient in Miami who testified openly in court. His name is Juan Molina. He's a Medicare beneficiary. He's been taking kickbacks for quite a long time and he says, you know, a lot of people in the community take kickbacks. They'd get a hundred or two hundred dollars a month to go give their card away. And he was a prime example of how this works. He says, "I went in and met with the DME owner. She paid me cash. I gave her all the information. The last I heard of her, I got all kinds of medicine billed to Medicare. They paid for it." And when the agents of the FBI approached him, after some lengthy conversation, he admitted that he didn't need any of that stuff. Well, when we looked at his Medicare data, that first company where he sold his ID was really the tip of the iceberg because once his identification information was in the system, we found six other companies that were doing the same or similar things with his information. And what was interesting is this, we went back and looked at the hotline calls and Mr. Molina was calling the other companies in and saying, "I didn't get this. I didn't get this." The one that was paying him, he didn't call about. And when we asked him about it, he said, "Yeah, but these other companies weren't paying me kickbacks."
So, we do have a problem and we're trying to use our resources within the department to address it effectively but we need to change the technology and get out in front of it and we need to use our resources to make it so that people who do this are appropriately sentenced.

>>Jodi Daniel
Right. We have a couple more questions that have come in for the panel.
I suspect that we've touched on some of this but the health consequences of medical identity theft can be profound and tragic. Are data available on the frequency of medical errors resulting from medical identity theft?

>>Pam Dixon
This is Pam. I don't think there's any systematic data that I know of.
There's a lot of anecdotal data and some of us are compiling that but in terms of saying, here's a national survey and here's a really good, solid number, plus or minus, you know, three error points, I don't think we have our hands on that yet.
I wish we did.   I think that one of the problems here is that it would require a lot of individual patients getting a hold of their healthcare records and going through

their records and then reporting it. The U.S. PIRG, a credit report, an accuracy study--do you remember that report, Betsy?

>>Betsy Broder
Yeah.

>>Pam Dixon
And it was a really fantastic report. They got individual--just individuals.
I forgot the sample size but it was in the thousands and they went, and they got their own credit reports. They checked on the accuracy and then they got an accuracy rating on the Credit Bureau reports. We would have to do something very much like that. And then, the problem with healthcare records that we do not have with credit bureau reports is healthcare records can reside in so many more places so we might not get the entire universe. We might not have the whole pie. With this particular crime, we're not looking at one pie; we're looking at a bakery. So, that's the problem.

>>Betsy Broder
It's true. There are three credit reporting agencies we can go to and basically, you're going to find most of the information there. But how many health providers are there throughout the United States? It would be impossible to know where that information resides.

>>Jodi Daniel
We have another question here. Somebody asked if there's any data on the average loss of a single incident of medical identity theft.

>>Pam Dixon
Yeah. I think there is now. I actually do think that those numbers are starting to come into focus. I think the--I don't know if you're addressing that in the atmospheric report, that might be in there, but we're seeing a range of anywhere from $2,000 to around $250,000. That's the range. We're starting to narrow in on an average at this point, though, and I'm not willing to share it until I'm really sure of it.

>>Jodi Daniel
Okay, this was a question for Shanda Brown. Clearly, the lack of affordable insurance is a key motivator, are you seeing fewer cases in Massachusetts' healthcare reform initiative that covers more people?

>>Shanda Brown
We're actually seeing cases where people are coming forward, at this point in time, saying, "I didn't have insurance so I was using this fake ID. Now that I have insurance, can you put those together?" So, you know, part of our uptake has been people actually coming forward at this point in time, confessing to, you

know, doing this in the past and now wanting their information combined into one record under their true identity.

>>Jodi Daniel
That's very fascinating. Somebody has asked about the source of any of the statistics that we're hearing and whether citations for these will be made available. If--do folks either have the information on their websites or can we--I don't know if we'll be able to pull that all together for folks after the conference on our website.

>>Betsy Broder
I think we probably have them on there. And our survey data, the FTC survey data, is available at FTC.gov/IDtheft under resources. And the breach information from the identity theft resource center is on our website. Just Google identity theft resource center and you'll find it.

>>Lisa Gallagher
And the HIMSS survey will be formally released on October 28 and will be available on our website.

>>Pam Dixon
Our identity theft report is available on our medical identity theft page.
And also, I have a PDF document of all of our resources. It's about three pages of resources and data, etcetera. I have it on PDF. I can mail it to you. I have it on paper here so, we can make copies and make it available.

>>Jodi Daniel
And we will try to follow up and get a resource list for folks as well so we can--oh, we have a resource list in the packet so you should have all of those websites in there. Thank you. And we will try to see if we can make information easier to find from our website. And with that, I'd like to thank our panelists for a very interesting discussion. We will now take a 15-minute break. There are some snacks outside and then we will come back promptly and start the next panel at 10:45.

Panel 2: Laws, Policies, and Procedures

>>Jodi Daniel
I would like to welcome our next set of panelists to--let me get to the right one--to talk about laws, policies and procedures that affect that of identity theft.
And as we did on the last panel, I'm just going to ask each of the speakers to state their name and organization very briefly and then we will get started on questions. All of the bios are in your packets and available on the website.
I also want to just let folks know again that we will be asking for questions during the course of the presentation; you can write them on your index cards or the folks on the web can submit them by the web. I ask that you please keep your

name and organization so we have some contacts for the question if you don't mind. And I also want to let folks know, if you didn't get your question answered at the last session, we've held some of the questions because we thought they might be more relevant or better answer by somebody on a different panel.
So we still have these questions and we hope to get to them. We may not get to all of the questions today because there are a lot of folks participating and a limited amount of time. So, with that, I would like to welcome our next panel.
Harry if you don't mind starting introductions.

>>Harry Rhodes
Thank you. I'm Harry Rhodes the Director of Practice Leadership for the American Health Information Management Association.

>>Jonathan Cantor
Good morning, I'm Jonathan Cantor I'm the Executive Director for Privacy and Disclosure at the U.S. Social Security Administration.

>>Gary Cantrell
Hi, I'm Gary Cantrell; I'm with the U.S Department of Health and Human Services, Office of the Inspector General, Office of Investigations.
I'm the Director of Computer Forensics and Investigative Research.

>>Marcy Wilder
Hi I'm Marcy Wilder with the law firm of Hogan & Hartson and former Deputy General Counsel of the Department of Health and Human Services.

>>Shanda Brown
Hi, I'm Shanda Brown; I'm with Massachusetts General Hospital and I'm with the unit that oversees our data integrity and medical identity theft response.

>>Stephanie Kaisler
Hi, I'm Stephanie Kaisler; I'm standing in for Kim Brandt, I work at the Centers for Medicare and Medicaid Services. I'm the Acting Director of the Division of MMA Integrity which is a really long way of saying "I fight fraud in Part D".

>>Jodi Daniel
I'm going to--just like last time, we're going to have a facilitated discussion.
I will likely direct a question at a particular individual or individuals but if folks on the panel have something they want to contribute, feel free to jump in, I would like to make this as interactive as possible. First off, Harry can you start us off by talking about some of the policies, procedures and laws that are currently in place to help protect health information based on your most recent white paper that AHIMA has done and what you've learned.

>>Harry Rhodes

Would be glad to. I want to frame my response by first saying that the very first thing you should be doing is a security risk assessment and that's what's very important before you can decide what tools you're going to select. And when you are selecting tools, it should be driven by what sort of threat you're facing and your assessment should help you identify--and your assessment should be ongoing so it would help you identify what your threats are now and what they are as you go forward. And you should realize that this is multi-task--as a previous panel said, that it is the one-off--it is the insider, it is the individual who's involved in drug-seeking behavior. And then when you realize--when you decide what you want to do and choose a tool, you need to realize that security administration is not just the IT solution; it is administrative which is training, education and also policies and procedures; it's technical which is all the [whiz-bang] IT stuff that's out there; and it's also physical… it's as simple as locking a door, as having a camera, it's as simple as having somebody just sitting there in the room watching the room and being aware of who's in the room with you and that sort of stuff. And then you need to be careful that you don't cause a bigger problem when you choose your solution--and by this, I mean, you see situations where they're screening patients for patient identification as they're coming in. The person who is doing it isn't even looking at you, they're just grabbing your driver's license, your insurance cards, spinning it around, putting on a copying machine and then placing the copy in the drawer right underneath the counter where people have actually reached across the counter and grabbed a handful. Either that or they gat really sophisticated and they decide they're going to do a digital scanning of your driver's license and your insurance card, which I call the 'picnic basket approach' and then they don't bother to implement any sort of security controls on the database and it's just like a picnic basket to the individual who wants that information; they can go in there and get it. Those are some of the problems that you may face. I want to comment on the earlier comment about the people who go into facilities and ask for--ask to see their information and are refused or not allowed to see their information, and when I was first a student of Information Security, one of the first things I learned was the CIA triangle… it's confidentiality, integrity and availability. Integrity of the record is not any less than confidentiality; it's just important and I believe that anyone trying to clean up the integrity of the record would definitely involve the consumer in doing that and I kind of suspect from listening to the comments from the Department of Justice gentleman that perhaps the individual--if you go into facility and you ask to see your record and they don't want to let you see your record, there's a good chance that they maybe the one who's actually committing the crime. And what we need to do is empower the consumer to go--be able to go somewhere else because this is an insider crime a lot of the time and the very people who are crowding the doorway and watching the gateway could be the actual people who are--don't want to be discovered and so they can throw up, "Oh, HIPAA won't allow us to do that," and I think that's a valid excuse. I do believe that there are things you can do and of course the HIPAA security and privacy rules are great place to start but, beyond that, I think that you should be investigating the Health Level 7 standards, HL7… the EHR functional model has a whole section on

security and then there's work being done by their role-based access committee and a lot of other committees. There's publication--standard publications by the American Society of Testing Material, ASTM, the work of the E31 group; there's some excellent stuff out there from the National Institute of Standards and Technology, NIST. There are some great work that's being done by the Health Information Technology Standards Panel, HITSP--point you to the TN900 document, this is the Privacy and Security Document, and also the contracts that go along with that. The work of the Integrated for Healthcare Enterprise, IHE… and even though it's considered European, there's lots of good advice there in international standard--International Organization for Standardization, ISO.
And then as far as professional associations go, I encourage you to go to AHIMA; we have a wealth of information out there, it's totally free, like we have a checklist for providers and also for consumers as what to do, step-by-step so you don't forget anything. We have publications such as our medical identity theft book and we're constantly adding to that. There's also the great stuff that Lisa mentioned on the HIMSS, Health Information Management and Systems Society, and I also encourage you to get outside of healthcare and look at such organizations as the Information Systems Security Association, the ISSA… that's a great place to go if you're looking for how to implement security, administrative, technical and physical control.

>>Jodi Daniel
Marcy, there has been a couple of mentions by Harry and some folks on the earlier panel about HIPAA and other laws that play roles here; can you just give a brief overview of some of the laws that are important and some of the comments that have come out about how the privacy role might act as a barrier to access records and whether or not that's true.

>>Marcy Wilder
Yes. I think that there are--probably the two most important laws right now on the health side in terms of protecting against medical identity theft are HIPAA and the state data breach notification laws. I also think that the red flag rules are going to be helpful. In terms of the relevant provisions of HIPAA, I think that the fact that patients have a right to access their records, the fact that patients have a right to request amendments to their records… health patients or consumers think that there are requirements placed on the covered entities, for example, to authenticate folks to whom they are disclosing records. And the security rule actually requires that, when there is some sort of a breach, that those incidents be addressed. So there are some rules in place although there are gaps. In terms of HIPAA and the questions that have come up, my understanding is there's an issue about--if there is information in somebody's record about somebody else, that some believe that record cannot be disclosed to the individual and I think that is simply wrong. And I think it's wrong for two reasons: one, that information is in the individual's medical record and the individual has a right to see what's in their medical record. Part of that transparency is precisely so that the individual can identify if there is something wrong or if somebody

else’s information has been somehow intermingled with theirs. So one is that disclosure is permitted because it’s part of the individual’s records; I would say it should be encouraged because it’s part of the individual’s record. And that, second, even if there was some concern that it would be a disclosure of some--an impermissible disclosure of someone else’s information--at the end of the day, that information as it relates to somebody else, is de-identified. So, that information is not connected or likely de-identified, not connected to another individual’s, so you are not unlawfully disclosing. If, in fact, even if it is identifiable, I would say it is an incidental disclosure concomitant with the permissible disclosure. So I think that there are any--one, I think it’s permissible. Two, if somebody says it’s impermissible, I think that there are a number of good defenses if challenged; although it’s even a little bit difficult to imagine what that challenge would look like or the individual would complain to OCR and write, “And I committed fraud and, as a result, my record was disclosed to an individual to whom I committed a fraud.” I mean it could happen, but I think that it wouldn’t be a problem. So that’s HIPAA. The second set of laws that I think are actually quite important are the state data breach notification laws. And that is because it provides the individual with notice--at least sometimes--when there has been a breach and when there is a risk of identity theft, and sometimes, of medical identity theft. Those laws which are in place in about 44 states require notification of an individual when there has been a security breach of unencrypted information involving usually a name and initials in combination with a Social Security number, a driver’s license, sometimes some other identifiers… credit card information or banking information. There are three states that add medical information to that list and those are California, Arkansas and Delaware. There is a lot of talk right now about whether or not at the federal level there ought to be a medical—one, a data breach notification law, and two, if which include medical information and we can talk about that later. It’s probably a good idea, at least a good idea to talk about.

>>Jodi Daniel
Stephanie, can you talk a little bit about CMS’s policies to protect health information and to identify where there might be incidents of medical identity theft?

>>Stephanie Kaisler
Sure, I’d be delighted to; thanks. When I think about identity theft, I think about the things that folks have said already but I think the crux of the matter is: people are our greatest vulnerability; no matter whether that person is the clerk at the giant pharmacy yelling someone’s name--we've been there--or that person is somebody who states that they’ve misunderstood the data protection requirements at CMS and they use some of our data systems for personal gain or the person who is trying to do their job very well put some data on a disc and it isn’t properly encrypted. So, as we go through this process, I think that’s one of the things that’s the hardest for folks to understand are that we all need to be ever vigilant. I'm not going to go over what others have said, but I think when it

comes to CMS… all of our contractors, as you know--and some of you were in the room--have to pass fairly stringent security requirements when it comes to beneficiary data. In addition to that, we on the fraud side understand that our beneficiaries may not be the most nimble when it comes to understanding anything from what button to press on the telephone when they're listening to 1-800 Medicare to understanding how to--they may not even have a computer to know what to do there. So what we do, at least with the medics--the Medicare drug integrity contractors, that's who I work with to fight fraud in part D--we regularly send out fraud alerts or press releases, we have on our websites messages about being careful, there is, you know, a document--and I know not everybody reads these things--but protect your Medicare number, your identity and your money. One of the places where we have found, I think, the greatest breach and the most public breach, is through something that we have called the 299 Scams. And you all have heard something like this… someone calls a senior and says, "Hey, this new Part D thing, it's expensive, but you know what? I can offer you free Medicare for life and all you prescriptions covered if you give me your account information or if you just give me your check information and we will take care of that for you." And, you know, it sounds pretty good. And so one of the things that the medic does is work with those beneficiaries to help them recoup their money but, in addition to that, sort through with the OIG--your folks--as well as the folks from the FTC to try and figure out how to do this. These are people who set up these call centers; they are nomadic and they are slick. Many of them are Canadian and their places of business are along the borders so they can disappear quickly from notice. I think it would be fair to say that there probably need to be--we probably need to be doing a lot more, and we plan on doing more. But I think one of the interesting things in this field--and I'm sure one of the reasons why you guys, I assume are intellectually curious on what you do--is that the people who are perpetuating the fraud against our beneficiaries are quite bright and they come up with new ideas every day and we have to try and keep up with them. So having said that, I'm not so sure that that's necessarily a discussion of procedures as much as what we've seen but I hope that meets what you were looking for today. Thanks.

>>Jodi Daniel
I would like to stick with the issue of policies and procedures and--but switch to what are some of the policy gaps or the security gaps that are--that people see, and what can be done to close them of those gaps? Shanda, do you want to take a first stab at that?

>>Shanda Brown
Sure, I think for us from a provider standpoint, one of the biggest gaps we have is we're just not sure who to report to in a case, you know… as a single facility, we have policies and procedures in place on how to handle this; we've actually acted pretty proactively in terms of setting up a one unique sourcement facility to handle any calls, any complaints to the investigation. We have a data integrity team in place that's multi-disciplinary so we have people from police and

security, we have people from IS, we have people from the clinical side, and we all act together when we get notified that we do have a potential a medical identity theft issue. So in terms of handling it internally, were good to the point that we've fixed it; we've sent out a notification to the patient if we think it's necessary and then it's kind of where do we go from there? So it sort of ends at the provider level. You know, in terms of gaining access into a big network of people to, you know, get some resources from that--sort of we have this issue of not being sure who to go to if we do have a deeper issue or bigger issue.

>>Stephanie Kaisler
Well, I think I can actually help there if you have faith in me to try.

>>Jodi Daniel
Go right ahead.

>>Stephanie Kaisler
I think, in the case, if you are working on Medicare, if it is a Medicare situation… we have contractors that fight fraud--program safeguard contractors in the fee-for-service world or, as I like to say, everything but managed care. And then we have the medics for managed care. There are phone numbers available… 1-800 Medicare is one of the easiest ways and that's the safest way, I think, for folks to just say, "We have a problem and we need some help." And the others, the OIG--I'm sure Gary's going to be talking about that--but there is also always the OIG hotline for you to turn to. And there are rather intricate procedures in place for how the information is taken in, how an investigation proceeds and then how it moves on to law enforcement; and it would be viewed, I think, as a partnering for folks like you who don't have your own Special Investigative Unit and things like that.

>>Jodi Daniel
Gary, do you want to follow up on that?

>>Gary Cantrell
Yes, certainly, we do work a lot with the CMS and CMS contractors in evaluating and receiving allegations of healthcare fraud. Healthcare fraud is really the majority of our work in the Office Investigations and this is a piece of it.
But what I want to kind of reiterate are some things that Kirk mentioned in the first panel and we're coming at it from a similar perspective, of course. He's a prosecuting attorney and we're the investigative agency that's looking into this and we're referring it for prosecution. And the aspect I want to point to is the provider side of this issue and the amount of money that's available through these fraud schemes and how quickly they can steal from us. What makes it so enticing, I think, and makes a larger vulnerability is that there is money to be made and made quickly in large sums and, in many cases recently, we are seeing provider's identities which are being stolen, clinics that are being opened under their names without their knowledge and they are able to find out all the

information they need, virtually all the information they need off of the internet, places like the NPI registry that provides all sorts of information about providers including their full names, their addresses, their businesses, their UPIN, their NPI provider numbers, their specialty type. All you need is a couple more pieces of information to send the fax or make a telephone call to the Medicare contractor to find--to create a new facility, obtain a new provider number and start billing pretty much immediately. So, and what we've seen in some instances is they gather up as much information they can, they reach out similar to any milk fishing and you guys know e-mail scams or were they ask you to log-in to a website. Basically this folks will call or fax information to the provider's office, ask for those missing pieces of information saying that they are from Medicare, ask for that SSN and that DOB for that medical license number if isn't available. Once they get that, they submit the application; open up a new staff service. And as Kirk mentioned within months 90 days they are able to build hundreds of thousands of dollars in some cases millions of dollars and by the time we've been notified that the incidence occurred, they may have moved on, close that shop talking about addresses that are vacant, and there's never been a business set up there. So there's--it's a quick hit and it makes it very important for providers to be vigilant and taking their own information so that isn't misused because it certainly enticement when you can get money quickly to the other side of that is you have to have the beneficiary--take numbers in order to bill. So, that another reason to go after that and you can do that through the methods that are already been described before. But the--we're probably seeing the tip of the iceberg in this thing and our focus within the federal investigation system in the past three years our piece of it and we work with FBI state medicated for our control units, U.S attorneys office and many other law enforcement agencies who have pieces of this information but just in our cases we've had three billion dollars in restitutions fines, penalties, settlement agreements in the last two years. And over 2 billion dollars before that and that's just like I said it's probably the tip of the iceberg. We don't have a very good understanding on the scope of Medicare fraud and healthcare fraud in general, much less at this point of the scope of medical identity theft.

>>Jodi Daniel
Can you, Gary talk about what are some of the things consumers and providers can do to protect their identity and prevent their identity from being stolen for these purposes.

>>Gary Cantrell
Sure, I think we need to reconsider making all the information that we do make available publicly on the internet, from a policy perspective and just cut that down to what's absolutely necessary to do our business. I think certainly providers should routinely check in with their--with the Medicare contractors to insure that the information that they have on them is accurate. These folks were able to transfer, and in some other cases, the electronic funds transfer destination from one bank account to the other. If they're not an active Medicare biller maybe they

don't know about this immediately but there's information that's out there they should confirm as accurate as well as looking at, you know, notices of payments and things like that shows what's been billed into their name and to--as best as you know, as best they can confirm that it's all legitimate.

>>Jodi Daniel
We've heard a couple of folks talk about these--very stiff identifiers including social security numbers and I think one person even talked about multiple people using the same social security number. I was wondering Jonathan if you can talk a little bit about--about the misuse of social security numbers and how to deal with that problem.

>>Jonathan Cantor
Sure well, as with everything in the identity area, social security number is a big component of identity theft certainly no different in medical identity theft. You know the history of how the social security number got to move from the pure social security system where it's used for the retirement program, the disability program and supplemental security income program into Medicare and Medicaid programs through national legislation and from there because of the close tie with the same providers. And the Medicare claims into the regular claim looks like naturally migrated from there --and to the rest of the healthcare provider community because they were building under that tip number which is the social security number. So, there is a natural motion there of course if you would want to use the social security number. In a world of financial identity after it was decided a long time ago that the social security number was the key and as long as the, you know--you don't even continues to use the social security number and Medicare. In medical community it's going to continue to service that e-function there as well.

>>Jodi Daniel
Shanda, can you talk about some of the things that providers are doing to try to prevent. Some of the procedures and policies that providers have in placed to prevent identity theft like complete training or some strained measures and place and a like.

>>Shanda Brown
Sure. Speaking from our clinic, we've pretty much activated a multi-fraud attack plan as it worked for this. Part of it is a robust training, on the intakes I do sort of have our staff beware of those triggers both during initial training and we do, do training throughout the hospital. Just so the staff is really aware of sort of this red flag kind of things, as you would say. That's the plan on how to deal with potential issue once it is discovered. So, who to contact, the next steps to take, we have a multi disciplinary team that was put together to handle those so we can nip things in the bud as quickly as possible. Our goal is, once we've got in notice about this is to pretty much get in attacking place and really start mitigating for the damage within 24 hours. In terms of cleaning up and in terms of you

know, some of the issues that have been mentioned with requesting a copy of the records. We have a patient index unit who access on--sort of hand holder for the patient where we do in the process of our investigation once we've confirmed this is the identity stuff, we will notify the patient that was the victim. If that patient does get back in touch with us, will sit down and will ask him about their history, you know, allergies. Since we don't have rules you're the record, with the hope providing them with the copy of the clean record and then they can let us know if there's anything that we've missed in the record so we do try to comprehensively handle from start to finish the entire situation.

>>Jodi Daniel
And how much do you see patients sort of being proactive in trying to address this as versus you really bring them in and they are the ones who identifying that there's a problem and that they need to sort of clean up their records and their financial situation.

>>Shanda Brown
I think--it's a situation that's out there in, you know, the patients mind, one of the problems is one things we have to put in places, we've got a patient who calls and you know, I have been in mentioned medical identities fast and--didn't even stolen, somebody's wrong information and will kind of had to stop and start our investigation process and find out sometimes pretty quickly that it was a wrong entry causing the situation. So I think that the public is becoming a lot more aware of the issue of medical identity stuff, were getting more calls of people that are using that catch race than we have them in the past. And I also think that part of that is you know, you have to be able to investigate, you make sure it's really that issue or not that simple, you know, or an error on the part of the facility.

>>Jodi Daniel
Stephanie, can you talk a little bit about how--any outreach that CMS has to consumers about taking corrective rules to--for their own protections.
You mentioned about protecting their Medicare number. Can you talk about a little more about any of that kind of outreach to consumers to protect themselves?

>>Stephanie Kaisler
There's a multifaceted program to be in touch with beneficiaries to help them understand how to protect themselves from this. And it is everything from the typical outreach that you hear about in Medicare where, you know, there's the big RV that shows up. We've got the regional offices have their outreach programs as I mentioned there are press releases and pamphlets, and then we do town hall meetings. We work very closely with the senior Medicare patrol as well as so that we can get the word out as quickly as possible.
To follow on the question that you asked Shanda about how are you hearing this and what is the percentage. I think for a new program like Part D, we are hearing from beneficiaries who get their explanations of benefits and well, usually don't

understand it, but then cannot quite figure it out where the medications came from that are on the list.
We aim to do more; we are working very closely with the managed care organizations. As well as the different carriers on the fee for service sign to do that.

>>Jodi Daniel
We've also heard some comments and I know AHIMA has brought out a point that the issues are not just about information and accurate information getting in a medical record but some of the secondary use of information and how inaccurate information can affect some of those secondary users as well.
Harry can you talk a little bit more about that issue?

>>Harry Rhodes
We brought together electronic health information measurement worker to publish a practice service guidance for individuals whose trying to prevent detect and litigate this, and when the groups tried to put a frame around this and what we came up was what we call the medical identity theft waterfall. We have a graphic of that, it's attached to the practice briefing it's on the--our website.
What we found was--first if there is somebody stealing your information and then you're violated with someone having to using it to sending a false claim and taking advantage of your benefits but then it--because of real penalty mentioned that hundred and fifty people look at your record but among those hundred and fifty people look at your record are those who used the information to make decisions. The pair who uses the information for pricing and for staffing and for determining what sort of benefits we're going to offer. It is reported in various research studies and it gets reported in various public health studies and so, the bad information gets out there and spread around and once it gets out there it's very difficult to get it back. A health information manager who I worked for 18 years and in facilities before I--with work for AHIMA, personally--I've--personal experience were people would question the data you've got back from studies because they said these figures are too high or too low or were mostly too high. And when you went in there you found out there was something wrong with the values. It's what the criminal will do if he finds a pathway that's going to get them what they want--for example the gentleman from the Department of Justice said earlier that they find something that's the easiest way in, and they'll keep going that and then what you'll see, is you see situations were you couldn't possibly had this when you diagnose this in this community. There is a cascading effect and once it gets out there it's very hard to get back and by now even electronic health workers that we have, we are working on interoperability at the standards level and we are working at a way to track information back to the parent document but we still got a ways to go there so a lot of times you give out the information in electronic form and there's no way to find out where the source is and that's we can definitely do and there are people working on that solution right now.

>>Jodi Daniel
Jonathan did you have something to say?

>>Jonathan Cantor
Yeah. I mean one of the--sorry. One of the secondary users in many cases is social security. If an individual turns around and files for a disability benefit, we often, regularly collect a great deal of medical information from providers throughout your entire medical history. We ask you all kinds of questions gather all kinds of information about your providers and go gather all kinds of service record. And other things we've certainly seen are cases where there are medical records that the claimant in this case has no idea what they are. Now, social security is, you know, five levels before final determination is made before we proceed in the court. So the claimant in this case was the patient before the providers that's multiple opportunities to review those records but we've heard at all level of the social security adjudication process where the claimant has said and of course this will interfere and slow down your disability determination because if you have records that clearly indicate that you are disable but then there are, you know, records that contradict that somebody's going to put the break on and start asking questions and that may interfere with might have been an easy case. And so there was an easy case where as you would have gone disability which would have, you know, helped you as a claimant where you would start to get your benefit checks but it would also take the burden off of others in the community who, you know, might be paying private disability insurance in the meantime. So we've definitely seen it. Now, the due process controls built in and social security may well be a model for others to follow, in some ways it might not be; but certainly for us we caught a lot of these things, but it creates a great deal of inconvenience because that same information will continue to show up as we work with providers down the road. We'll continue to see that same information because it's coming from, you know, an unknown source that were not able to pick up it's just in your record. As you've certainly seen more of this with electronic health records that we've seen the traditional health record. That being said we continue to see great advantages to help information technology in the sense that it will help us in the transition and move things through the system faster but we have notice problems with inaccuracies in the records continuing to repeat that itself. And it has a researcher and also a security as well with the large research agency on top of that. The feasibility functions, you know, you would see in those type of problems. When you have contradictory information, you might have to throw it out from your sample too.

>>Jodi Daniel
How long can that--that can be a delay is for somebody who has disputed information in that record and he's trying to get feasibility?

>>Jonathan Cantor
You mean how long is the feasibility process?

>>Jodi Daniel
No. How much longer will--what is the range that somebody could expect if they have information that is inaccurate in that record and that is undisputed? Would you be booking for the feasibility claim?

>>Jonathan Cantor
Basically speaking, when the limit, you know, when that was uneasy situation and the case it should move very quickly through the system because it's clear type individual who's disable and no longer capable, substantial gain for activity. Is when you see those contradictory records, you have to build back to that claim. And instead of giving in that step one that initial state of determination and have to go back in interview to claim and ask for more information. Interview them about that provider and it's when they're dealing with that person across the often it was a state level or it was also the security office saying," I have no idea what that information is. And that the boy is now obligated to do a little bit of intelligence." So, we could slow it down depending on you know, if it's not so clear type, you know, it may end up before a judge crime determined whether or not it really is. You know we have the victim from the last panel who has the same name. Okay, so you can probably move very quickly but in some cases it can really sworn out the process. And basically, harm in the individual, that is how that issues being work out.

>>Jodi Daniel
I'd like to turn back again to talking about the individual. Marcy, let's start talking about the state breach of notification laws in some of the states, privacy laws and consumer protection laws. Can you talk a little bit more about of how these breach protection of laws work when somebody needs to be notified and what that means for a consumer who is getting this notification?

>>Marcy Wilder
Sure, so it talk a little before about the circumstances on which notification is required. I'd talk about the elements usually the name, excuse me, and initials in combination with social security number, credit card information and in three states, medical information. Many times, however, when a breach occurs in a medical context, there is no notification is required for example, if sometimes their social security numbers included in claims records, that's increasingly less the case, but it still is apparently feel open the case. And when those numbers are there are folks are notified that one there's risk of identify theft but--of financial identify theft but also that medical records were involved. Now, once that happens, there's a real question, and if you look at California, California's currently struggling with the question of what we'll tell folks, once they've been notified that their medical identities are at risk. Because, I think, some folks on the former panel spoke about, there are very clear cut step you can take to protect your financial identity. There are not clear cut steps you can take to protect your medical identity. There are some for example, when you tell people, what you should do is really look carefully your explanation of benefits. They will

often say it's you, "I have looked carefully at it and I have no idea what it says." Now that is, there are number of problems, I think that can and probably will be solved in the future as health IT comes a--is it of a--is more widely adapted and gets better. And provides enhance access to consumers for their records.

So, you know, right now, what folks can do is look at their EOBs, look at their records, try and see if there has been some kind of corruption of those records. And then, usually what they'll do is talk to their provider or their health plan and there maybe some assistance available. But really there are not a whole lot of good answers right now because even if you correct your record with one provider, there's not a great way to correct all of your providers or even though there are places where information is aggregated, for example, your prescription records are aggregated right now. But consumers don't have access to the places where they are aggregated. And so, it's very difficult to correct at that level.

In addition, once you do correct the record, I hear quite often that, "Well, I did ask from my records to be for them to delete the wrong information but they won't delete it they'll simply put a note on the file that says that information is wrong." Now, there are actually good reasons that providers do that, the question becomes from a consumer's perspective I think, "Is there a better way, okay, if you're not going to delete the information, is there some way to make it more clear that information shouldn't be there." And I think again, electronic records as those standards are develop, or to take account of what those amendments should look like. So, it's not a footnote at the end of the file but rather that block is grey or a different color or, you know, there are number of ways to flag, for a provider, that that information should not be there without actually deleting it.

I mean, another set of issues that I think--and I think the standards organizations are aware of this and are working on it for a number of reasons--but, you know, audit trails and source codes are tools that will be very useful to a consumer in terms of correcting the record. Those things are really at the early stages right now, they're not particularly sophisticated and even where they are sophisticated they haven't been adopted. So, I think we are in a transition period right now; I think that there are some steps consumers can take but that this is an area where technology can really help.

>>Harry Rhodes

I wanted to respond to some of the comments you made. As a health information manager, I need to point out that the health record is a business record and for that reason, because it's a business record, you don't want it to look like you've been pulling stuff out. And so, in the paper record, it's very hard to pull things out. And then, usually, you use every bit of space because you don't want to waste paper and so there's no space to write in the margins or anything like that. So, yes, it does come at the end, but there are some solutions that are out there right now. One for example is the HL7 version 2.5; there's a recommendation where you actually would take the document out and put it into a separate directory and then you put an HL7 message that points to the information of the directory and the person is using the record doesn't see the erroneous entry, what they--all they will see is a flag, an HL7 flag which would send them to a separate directory where the information is. And ASTM also has a similar recommendation with that as well. Some of the things I want to say--from my personal experience, I have Blue Cross and Blue Shield in Illinois and they have a thing called [Blue Connects] where, if you sign up for it and it is voluntary, you--whenever a claim is filed, you get an e-mail and you go to their website and see that a claim has been filed and I realized that that's after the fact, but still, it's a way… if you do respond it, if you are encouraged to respond to it, then you can point out to the payer that something is not right in it and even look into that. And the other thing, I've--I was involved in AHIMA because you wrote an article about this but there was an initiative called the PICASSO and it was a National Library of Medicine-funded grant with Science Application international in the University of California, San Diego and it stands for Patient-Centered Access To Secure Systems Online. And basically, what it was, it allowed the patient to go online and view who was allowed to see the records and, you know, see who was looking at the records. And so they have a list of everybody that was allowed to see, but they also got to see who wasn't allowed. And in addition to that, it allowed the consumer to go in there and tailor it so that they could get e-mail messaging whenever the certain parameters were met. So if you say, "I want to see every time somebody looks at my record that isn't on the list," you will get an e-mail. And then you can go any time yourself and look. And also in addition, you could say, "I'm not in the hospital right now; if anybody's looking at my records, send me an e-mail," I thought it was a great idea back in the mid-90s; I still think it's a great idea, that's something you can do.

>>Jodi Daniel
How difficult are those technical solutions that you're talking about?

>>Harry Rhodes
Well, I'm only an IT guy on the edge. Okay, that so, you know, I'm sure that all of the technology that allows you to do that is readily available. I mean, it's just a tickler system and you put in trigger and when you account for the triggers and if the trigger is initiated then the machine just sends you the e-mail and it's up to you to act on it.

>>Jodi Daniel
Can you talk into the mic so folks over here can hear? I'm just curious; the system that you were just talking about, PICASSO, I'm just curious if, for example, the individual authorized that somehow to go to a third party. For example, say, they vouch for this building or something like that.
I mean, obviously that wouldn't provide that tickle for when those people accessed it. And then, of course, if we moved it to another third party or fourth party, it would only be that one time. It would only be the title that they set it up for.

>>Harry Rhodes
There are some limitations to it but it is still a way for the consumer to get involved in monitoring who's looking at their health records and they would get a better idea who is on the list and who shouldn't be on the list. And yeah, there would probably be--like Shanda said, there would be a lot of times where you chase after something and it'd be something totally legitimate but at least you'd have somebody looking at it. I mean, my biggest concern about the whole thing, I've worked in Texas and Oklahoma before I came to work in Illinois and there's a phrase down there that says, "Closing the crowd gate after the horse gets out," and in a lot of ways, that kind of a system, you know, the person has already gotten there and got the information and now you're going in to close the crowd gate after the horses are out. But I mean, there's still a way because these are not isolated--you know, usually part of the bigger plan and so if you were lucky enough to identify something that was going on early on then you could probably intercede and do something and that's why I think there is some value in that; I don't think it's the begin and end-all solution. No, I wasn't suggesting that; I was just kind of curious about informing people while they're using a system like that if, you know, it doesn't keep track of third-party disclosures that may have already occurred or that you're currently authorizing that, you know, weren't in that network. Okay, I think I've--from what I understand, what you're saying, I go right now HIPAA does require you to keep on accounting of disclosures that are outside TPO…treatment, payment and operations and so facilities right now are required to track all of those disclosures. From what I understand from the Med ID project then it's been a while since I worked on that article for our journal. They did keep track of everybody who was authorized either through treatment or payment or operations to view the record and then plus everyone who made a request and that's why I understood it. If they didn't, I think it would be a good idea; it would give the consumer a better idea who's looking at their records and for what reasons and who's looking at it and shouldn't be.

>> Jodi Daniel
Marcy, do you have something to add?

>>Marcy Wilder
Yeah, a couple of things. I think at this point in the conversation, we ought to introduce another concept because what's happening is--and this often happens in this discussion--well, more disclosure is better and consumers ought to know more about who's looking at their records which, as a high level of proposition may be true but, in the details, is oftentimes not a good idea because what happens is when you have over disclosure like with any early warning system… people are saying early warning is a good thing because people can do things to protect themselves. But every early warning system ought to have some controls built-in so that there are warnings only when there is danger. And I think what happens is when you start talking about over disclosure or notifying consumers too much, you start worrying people or giving people pause or making them jump

through hoops to protect themselves when, in fact, there is not any material threat of danger. And that's one of the conversations that need to happen with breach notification laws. One, should you notify when the data is encrypted; probably not and most states don't require it. Should you notify only when there is some reasonable risk, significant risk, material risk, pick your standard of harm. Probably there ought to be some trigger before you notify folks that there's been some kind of an incident and you can talk about what that standard should be. Last thing, in terms of the accounting of disclosure requirement, I do not think that that is the answer. Let me repeat that, the accounting of disclosure requirement in HIPAA right now is not a good tool to address medical identity of that and that's for a couple of reasons. One is the accounting of disclosure requirement do not require an accounting for disclosures made for treatment, payment and healthcare operations. I actually don't think it should, but if you look at medical identity theft, it is most often perpetrated by an insider and that type of a disclosure would not show up in an accounting. The second is, truth be told, given where technology is and systems are today, most covered entities have a great deal of difficulty keeping an accounting of disclosures; they try… some do, some don't but it's not a good tool. And so I think, we should move away from the concept of accounting of disclosures and think more about audit trails, how that's checked internally and at what point consumers ought to have access.
But I do think--I want to push back on the notion that disclosure and lots of it is the answer because I think it makes for a lot of unnecessary anxiety as opposed to an effective of early warning system where people can actually take action. That was the answer.

>>Jodi Daniel
We have a lot of questions here and this one I think, in the context of what you just said, might be taken out of context. But it says, Marcy's point of disclosure and transparency is the ideal. I think this was in comment to your conversation---to your comments about access. But in practice, it is not followed; who or where do you go to dispute the ability to see your medical records?
So, somebody does not provide access to records and you believe that you should have access to those records, what can a consumer do about that?

>>Marcy Wilder
Every covered entity is required to have a notice of privacy practices and I know all of you have saved them in a file at home. But in case your file has been misplaced, when you request the notice of--you can request the notice of privacy practices-- it has to be posted on their internet site--there is always, by law, a way to find out who to contact for privacy issues. And if you start with that contact, they will usually get you to the place where you need to go to address those kinds of concerns. In terms of--I also want to be clear that I was not arguing against transparency, I think transparency is a good thing, I think there need to be some controls around it. And I also think that personal health records, as they evolve, are also go to be a very useful tool in terms of creating

transparency and presenting information in ways that consumers can use and understand.

>>Jodi Daniel
Great, here's another question. And this is, again… what can consumers or victims do you, the question is, "Is there a single law enforcement point of contact in the non-Medicare cases that victims could call if they believe that they have been a victim of medical identity theft?

>>Harry Rhodes
Well, that's actually a problem that we uncovered in our EHIM work group that there's--people aren't sure whether they should go to the police, they aren't' sure whether they should call the insurance payer and report it to their fraud investigation team, they're not sure whether they should call the FTC.
They really don't know and, actually, do you think about the fact that these criminals work very quickly in 90-120 days; by the time you figure out where you're supposed to go… you know, it may be too late. A lot of people--I noticed it in conversations with our members and with the general public that call AHIMA, a lot of people don't even know who the Office of Civil Rights are but you still see people going to the Office of Civil Rights to report medical identity theft to them and I don't see that showing up on their quarterly reports or one of their reporting's. I don't what percentage of people is going to them with that problem. And so, there is a problem and the one thing that we try to do is we try to create a checklist for consumers but even our checklist has the website for the FTC, it has the, "Go to your state Attorney-General's Office, contact you local police or tell your providers. So you--we are telling you to go a lot of places because there's not a single phone call that you can make or single e-mail you can send right now.

>>Gary Cantrell
Let me add to that briefly. If you do call law enforcement officials, whether it be a local law enforcement official or the FBI or HHSOIG, most of us are working together on these issues and their task forces throughout the country and the information, I would expect in most cases, would get to the right place and the right investigative agencies. So I would encourage you just to answer that question to call any law enforcement that you have available to you where you can get someone to answer the phone and they will take it--take it from there. Including the HHSOIG fraud hotline which is 1800-HHS TIPS or clear that out there. We don't investigate every identity theft case; our area of responsibility relates to HHS programs so that's primarily Medicare, Medicaid, healthcare fraud cases but we would know how to get the information to the right people.

>>Jodi Daniel
So staying on the theme of consumer protection and what consumer can do… this is a good question… let anybody who feels that they want to take a stab at this, please do. There seems to be a gap in coverage between laws that protect

consumers against financial identity theft such as the Fair Credit Reporting Act which provides, for among another things, free credit reports and fraud alerts and HIPAA which does not provide for same levels of access by consumers. What is the best way to bridge that gap as legislation requires? Maybe we'll save this for the reactor panel as well, but …

>>Pam Dixon
I'll certainly; I'll certainly take a stab at it. One of the things, I would point out is that, you know, we've talked a lot about, we've heard a lot about that right now… there isn't really a centralized focus. And so, to me you have to take facts at it as they are. And so, just speaking as a citizen and an individual, my recommendation would certainly be go every different direction you can think of because the issue here is as Betsy pointed at this morning. There's a real risk of personal harm here, it's not just your pocketbook. Your pocketbook is the issue too. But there's a real risk of personal harm here. And so, my advice would be to go everywhere you can. Call your providers, go ahead contact your insurance company, call HHS OIG, call law enforcement, and call the FTC. I mean, go every possible place that can be thought of because, hopefully, you'll catch somewhere in the system. You can still call the credit reporting agencies and still place fraud alerts there because there is an identity theft going on.
So, those bills will probably eventually show up on your credit report.
Have that fraud alert there because, at least, it will keep the collection agents away from you. Go ahead, ask your providers for access, ask for an annual summary of your EOBs. Call those providers as soon as you see anything funny to it. Everything you can because at least that may help mitigate the risk in harm with you. I mean, I won't comment on whether legislation is necessary.
As federal official, then I would certainly suggest that you know, there's a gap then there's a gap. So, you know. No one has clear regulatory authority right here, so. I think, going back to the beginning as a problem I think it's still that consumer waste a lot of time, or looses a lot of time because they don't know where to go. And so they learning as they go and I've--I hear lots of stories… the average consumer spends between $800 to $5,000 pocket train to clean up their medical identity theft issue. And a lot of get totally pressure and hiring attorneys sometimes. They don't know where else to do because they just don't know about all hotlines and the. And there's as fears that they go to lock in prison and they don't care that they report to the insurance company. And they don't care and maybe then what they needed is the feedback because they run a job or working on it were all connected, and consumers are that, they're not getting that reassurance that, "Okay, I call somebody but he's probably sitting at someone's desk is what they tell me over the telephone and the e-mails, so they send us at AHIMA so..." I think that happy here where they were coordinating this and I think they need to help the consumer. Have a plan of action and encourage them to move quickly and that we need to reassure them that something is being done.

>>Jodi Daniel
Marcy?

>>Marcy Wilder
No, I think legislation is certainly one option and one that ought to be looked at. The question becomes, though, what kind of legislation because it may not be what you think. So it may be that the best thing we could do legislatively, in terms of medical identity theft, is not a--is not or in addition to some kind of a notification after the… Is focus on the rights that exist and how they need to be changed or strengthened in this new environment? So, for example, "Yes, you have the right to access your medical records." But you do not have a right to access your medicals electronically or in a format that is understandable to you. And that which is not doesn't directly go to the medical identity theft issue, may be something that will greatly enhance consumer's abilities--ability to protect themselves. So I think that--and I think, frankly, that we are go--we already seek…congress is already setting the table to address this issue as part of a set of other issues related to health IT. And so, that debate is going to go on.
And I think, frankly, we are going to this legislation, probably in 2009, it may take more than a year--that addresses this in some way so folks ought to be engaged in that.

>>Jodi Daniel
Great, we have a bunch of questions about Social Security numbers so I'm going to turn the tables a little bit and, Jonathan, you might have to answer a couple of questions. Not all of these… I would like some others to jump in, particularly this one. What should a provider do if they observed anomalous Social Security number use? For example, credit searches that are used by more than one person and it cannot be determined who the victim is and who is the legitimate owner of the Social Security number.

>>Shanda Brown
From a provider's standpoint, at that point in time, the first thing that we'd kind of want to do is remove that Social Security number so it can't be used moving forward. Then, you'd want to reach out to, you know, if we'd already sent out of the--or in that case, you know, we'd reach out for assistance like we've just been told in--you know.

>>Jodi Daniel
Can you talk into the mic a little more? Thank you.

>>Shanda Brown
Once we've acted internally to mitigate any sort of damage or mitigate any future use of that Social Security number, then we would want to reach out to CMS or Social Security to get a little more assistance and what to do moving toward. But I think that from a provider's standpoint, the first thing you want to do is to

remove that Social Security number so you're not running the risk of anybody using it until you can figure out who it actually belongs to.

>>Jodi Daniel
Okay. Jonathan, you have anything to add to that?

>>Jonathan Cantor
No, I mean, Social Security is an agency, when we interface with people, at least in the provider community, we tend to be a receiver of information. You know, we don't verify or provide any information outside the agency which enable, to doctors to medical providers because there's really, you know, you're getting into some of these core privacy principles about compatibility with the reasons that SSA collected and created the record. And in this case, we created the record for us to run the Social Security program and it gets difficult for us, because without an individual coming to us and saying, "I want you to, you know, verify my SSN for me," which, of course, we would do if the individual came to us. You know, our hands are kind of tied because we don't have the authority to go out proactively to that provider. I will say that our Inspector General and Social Security colleagues here, Gary, that they would be interested in any case where there's a lot of fraudulent use as a Social Security number, even a little bit, because they will often find, you know, "Where there's smoke there's fire."
And then of course, just like as Gary was pointing out, there's a lot of cooperation back-and-forth between inspector generals within agencies in cooperation with local state and federal law enforcement and so, you know, there's often a little bit more going on than just one misuse of that Social Security number that's being misused in one place is often being misused in other places.

>>Jodi Daniel
Well, this is a follow-up question from somebody else, but sort of follows on nicely. How does a provider or other entity move away from using Social Security numbers? Can they deploy a new number in convention and if so, how?

>>Shanda Brown
What we have contemplated looking into from a provider's standpoint was creating a unique ID that's an amount of different stable identifiers, be it certain digits from your Social Security number as well as, you know, mother's maiden name, you know, part of your date of birth, but things that don't change in using that amalgam is the unique personal ID number as opposed to just going back to a Social Security number. It's difficult because it is one of those things that… unfortunately, SSN is something that is a unique identifier for a person and trying to maintain, you know, patients' security and patients', you know, integrity as well as trying to identify patient is difficult.

>>Jonathan Cantor

Certainly, there is nothing in the Social Security Act, anything in the Social Security administration policy or regulation or rule that indicates that a provider must use the Social Security number. It's actually only mandatory for the Social Security Administration internally and there are certain federal and state programs that are required by law to collect it and are authorized to use it. There is no law requiring that they display it. So certainly, I--from where Social Security would sit it a provider network or a provider community or even the state wanted to use its own system and build while still complying with the law, there would be certainly nothing that we would say is the problem there.

>>Harry Rhodes

When I worked for a large healthcare corporation and we had regional master patient indexes and we made sure that no matter where the patient went in the region, that we could identify them by the number that we associated with them but, getting beyond numbers, what you could use is--what Shanda kind of alluded to is an algorithmic system where the system, when you're searching in the master patient index trying to find the patient you can pick up on the birthday, and mother's maiden name, you know, the gender, you know, the birth town, birth state, those kind of things where you can through an algorithm, you can narrow it down there and identify the patients that way and not necessarily use a number.

>>Jodi Daniel

Hmm, and this is one more follow up on this. It says, "CMS uses Social Security number as my identifier. Are there routine checks against the SSA death master file to check for fraudulent use of a dead person's Social Security number?"

>>Jonathan Cantor

We regularly provide them death data and we regularly provide CMS protective data from the states that's not available because this it's protected by a special provision of the social security act; it's not available through any other mechanism, even the Privacy Act or the Federal Freedom of Information Access. So CMS has a particularly unique file with that information.

>>Jodi Daniel

Marcy?

>>Marcy Wilder

Yeah, I also want to lay it for folks that, you know, the states regulate what you can and cannot do with Social Security numbers and many of them in particular say that if you are go--in certain circumstances, if you are going to use Social Security number as an identifier, even internally, then there are security protections that you are required to take. So they regulate when you can ask for it, how you can use it and what you need to do to protect it and those laws vary from state to state.

>>Jodi Daniel
Thank you. Next question, I think this is for Shanda. What procedure do you use to verify identity of a patient?

>>Shanda Brown
We do ask for a patient ID when the patient does come in. We don't get those at all times but we do take that information, we match against the patient's photo and our staff is being trained at this point in time to question, not interrogate, if they see some sort of difference in that information. We'll ask them to verify things like there is, you know, most recent stay that you would think this isn't the same patient, their condition. Again, not in an interrogatory way but, you know. So if we have out-of-state driver's license and we see the patient's been here recently so, you know, "So you're new to Boston? How about the Sox," you know that kind of thing. So we can try these to get their information if we suspect that they're not using the correct ID.

>>Jodi Daniel
And what do you do with the information that you collect on your patients just for purposes of identifying them because that was what came up for the last.

>>Shanda Brown
We do not collect a scan of that driver's license, we just ask the ID to verify so we don't actually--we're not actually collecting that information at this point in time.

>>Jodi Daniel
Okay, Harry?

>>Harry Rhodes
One of the things I've covered when we were doing our environmental scan to AHIMA was I was interviewing an individual who worked for a children's hospital and how they were identifying children that were trying to seek healthcare with somebody else's identity was a child would suddenly get taller or shorter or the eye color would change or anything. And so what they started doing was they had a registration system that allowed them to photograph the child and it did help to, you know… when you're sitting there and you're processing a child or registering them, you could look at the photo of the child and it did help you to identify those cases where people would try to use them, someone else's coverage for another child.

>>Jodi Daniel
This is a question for Harry.
Who is authorized to look at medical records? How do you determine, who is entitled to look at your medical record; it could be a large list.

>>Harry Rhodes

Well, certainly, the patient does sign authorizations to allow us to view their record. A lot of facilities, even when they're registering the patient, they ask them to sign a consent that allows the individuals who are involved in their treatment, payment and operations to view the records, you have to be aware that you have a current authorization or a current consent. You have to be aware that the person who is asking for the information has a right to view the information. Back when I was a director of the Medical Record Department of--I used to tell my staff that if you don't feel good about the request that is being made or the person who's making it, tell them "no" because it's a whole lot easier to deal with it and investigate who this person really is and whether they really should have access then to get the information back after you release it. That was kind of our policy, we did take a great deal of effort to make sure we had signed authorizations and that if there was an individual who had a legal authority like someone investigating child abuse or elder abuse, we've to make sure that that they had their IDs. And we did had situations that where people would come in with the briefcase and they're all dressed-up in a nice suit and everything and they'd want to see somebody's records and, you know, you knew it was a child abuse record or an elder abuse record and you'd ask for their ID if they actually from the state or the health department and they say, "It's out in the car," and you said, "I really can't let you see this," and then they would leave and not come back. So, you would assume that people, you know, did try and we're very diligent to make sure that we--we're not, you know, we were totally shameless, we would make phone calls and ask people to validate who they said they were and so we took it very serious.

>>Jodi Daniel
Okay, one more question here. To what extent does government authorities have access to data necessary to detect and prevent fraud and what is your wish list to improve Medicare/Medicaid fraud protection?

>>Gary Cantrell
I'll start out with that one.

>>Jodi Daniel
Remember, we're thinking about medical identity theft.

>>Gary Cantrell
Right, right. One of the challenges we have is a lot of the cases that we see are national in scope. And so, a lot of the data, repositories for the data, and the billing data for Medicare in particular, is stored at a regional level and not necessarily at a national level or if it is at a national level, it isn't available to us in a timely fashion. We would like to address these problems as quickly as we'd like. So, the wish list is, you know, National Medicare Claims Data that's accessible and timely as well as Medicaid data, that's another area where I know CMS is working to consolidate Medicaid data from throughout the country at a single source so that you can actually do some studies across the country,

across states, to identify, you know--for trends, fraud, whatever it is that they happen to be researching. So data availability at the national level is something that we're interested in from an investigate perspective. We do have data available to us, so it's not as we don't have it; we do get it from CMS contractors, we get it from CMS directly upon request, and we get it from providers when we issue subpoenas or, in some cases, search warrants. So data is made available to us, we always like it as quick as possible and certainly as much as we can get relevant to our investigation.

>>Stephanie Kaisler
I'd like to follow on that if I could.

>>Jodi Daniel
Please.

>>Stephanie Kaisler
Gary did a really good explanation of the fee for service side of Medicare.
But when it comes to managed care in Medicare, SSN also on the Medicaid side, it's much more difficult. In managed care and Medicare as you know, Medicare is not to insure and so there are hundreds upon hundreds of sponsors for Part C and D. And they do send in data but providing it on a national level in a system that is easy for people to use is, I guess, on my wish list. I also think that more data should probably be available to CMS than it is today.

>>Jodi Daniel
Okay, any last point from any of the members of our panel? Thank you very much, please join me in thanking the panelists. We will now take a lunch break, there are boxed lunches outside, there are fair share boxes for people who contribute and we will start promptly at 1:15, thank you.

>>John Loonsk
Good afternoon, everyone. My name is John Loonsk. I'm the Director for Inoperability and Standards in the Office of the National Coordinator, and I'm going to be leading this panel. We have a distinguished group of experts here. I want to say, for those of you who are on the webcast, I know a number of you have asked about parts of the webcast that may have been missing because of the earlier technical difficulties, and those will be recorded and will be made available on the web. So, if you've missed any parts of the earlier sessions, those will be available to later and accessible from the website. I'm going to turn to the panel and have them introduce themselves in a minute. As Jodi indicated earlier, the bios for all the panel members are in your packets. I just will have them identify themselves. This panel is about Health IT, and it's very hard to separate out the IT aspects versus the business aspects. We're going to try to focus on both the positive aspects of Health IT; what it can do to potentially help with medical identity theft issues, and we will also, at times, may be talk about some of the ways in which it facilitates the problem, and hopefully we can have a good

discussion of that. We will try to distinguish between the issues of one off's and systemic problem, and we will break our discussion down, principally, into three areas. We're going to talk about, particularly, Health IT and approaches, diving into detection of identity theft issues, then we will talk about response, and the steps and response, some of the issues in response, and then we will also talk about prevention and education and technical aspects of avoiding identity theft, moving forward. So with that, let me turn to the panel, and if we can start down there with you, Harry, just identify yourself and your affiliations, please.

>>Harry Rhodes
Good afternoon. My name's Harry Rhodes. And I am the Director of Practice of Leadership with the American Health Information Management Association.

>>Lory Wood
Hello, I'm Lory Wood and I'm the Chief Security and Compliance Officer for Good Health Network. We are a PHR vendor and identity proofing.

>>Liesa Jenkins
Hi, I'm Liesa Jenkins.
I'm the Executive Director of CareSpark, which is a Health Information Exhange in Northeastern Tennessee and Southwest Virginia.

>>Calvin Sneed
I'm Calvin Sneed with the Blue Cross Blue Shield Association.
Thanks for having us.

>>Lisa Gallagher
I'm Lisa Gallagher with Health Information and Management System Society.

>>Debbie Banik
And I'm Debbie Banik with the Indiana Health Information Exchange. I'm the Director of Clinical Messaging.

>>John Loonsk
Thank you, everyone. So, I've encouraged all the panelists to talk amongst themselves, and hopefully we can get a good discussion going. We're going to look at this from several different perspectives, and as you heard, have several different views on this issue representing these different organizations. We're going to start in detection and by talking with Calvin. And Calvin, maybe you could just make a few comments about, particularly, systemic detection and some of the things you're aware of that are being done from Health IT standpoint.

>>Calvin Sneed
I was hoping you'll start with a real expert.
I think most of you know that from the insurer perspective, we may actually be tiny bit ahead of some of the rush of the community, and there is a very good

reason for that. And that would be that we have customers that have to be made and kept happy, and customers want their premiums to stay down. So, the insurance side of business, you know, if you're not preventing and detecting and saving money, then you're not trying to keep premiums down. And so, for some years, you know, probably 10 or more years, there is a very significant vendor community that have been working on software detection systems for both the prepaid, from the prepaid side of claims, and the postpaid side of claim. Someone mentioned this morning that it's much cheaper to catch it on the front end and not have to pay the chase those dollars in the back end. So, in our community we try to emphasize that that's important thing to remember and keep in mind. The things that are done on both the front end and the back end, in that regard is using systems, detection systems to look for aberrant billing patterns, largely. You know, there're also claims edits of emplace in the industry to catch improbable or unlikely claims; for example, billing on holidays--things at a very basic level. The prepaid and postpaid software detection systems are paid pretty large dividends when they're turned on and when they're applied to the claims processing. You know, they basically spit out, you know, incongruent claims comparisons, and those things are then either handled at a basic, reactive way or if they're significant aberrancies, moved down the chain of command to or--yeah, the chain of command to researchers and investigators to determine the validity of the claims.

>>John Loonsk
Thank you. Surely, one can see that from a payer perspective there may be a good alignment of doing those, supporting those analyses. Is that true in the provider sector as well? Either Lisa, I guess, Liesa J., do you want to talk about--or either of you--talk about provider perspective and what's being done in the provider sector?

>>Lisa Gallagher
Well, I talk this morning a little bit about some of the data that we found on our survey and I'm going to reference that in a second. It seems to me that the incidence of medical identity theft that are detected and provider organizations are detected, sort of, in two ways. One, through the front prevention units--there we go--and in the hospital provider organization, and then another is on the security side, when there is a breach. So, with regard to the security monitoring side, you know, some of the technologies that are used that we see are intrusion detection devices, audit logs, those sorts of things, which collect data on the activity that is going on in the organization and can, help them determine if there's been a security breach. Of course that would then link into the activities of the security staff or the network IT staff who look at the logs and monitor the activity to see if there have been a security breaches. And then, of course, that breach would need--as I discussed this morning--to be linked to medical identity theft as a threat motivator. With regard to some of the data that we got from the survey, one of the questions that we asked was whether the organization monitors or audits proactively the care records so that they can confirm that

services are delivered only to the appropriate recipient. And, we had a response rate on that of 41.3%. Now, the course to me that some of that monitoring and auditing might be done on the quality or patient safety side of the house, and in that case, then we would also need to make those folks aware that, if they start to see some anomalies in their record that there's some coordination that needs to be done in the organization to link that data in that record to a medical identity theft issue as opposed to just an inadvertent error or, you know, a trend with regards to quality or patient safety. And now, I do think there is, you know, increased awareness about medical identity theft. I do think, however, that efforts tend to be, sort of, stove piped in the organization and maybe the approach that someone like Shanda did at Mass. General, where there is a coordinated approach in one office that deals with medical identity theft, might be a model for some of the providers.

>>John Loonsk
Harry?

>>Harry Rhodes
To add to that, what I've come across, I think, is a really positive thing going forward is some organizations that are going to an Electronic Health Record are establishing a job title of Data Integrity Specialist. And they're trying to make this person a very visible person so that people know about this individual or this team, and that they can come to them with issues that need to be addressed, because one of the things you always hear about is who has the time to do this, who has time to chase it down, but if you make it some, I guess, ownership for in their job role, then you'd have a better chance that they would devote time to it. Some of the things that they do, in a master patient index, they look for duplicate number issues, they look for number issues that don't look right, they look for misfiles and information, otherwise, information that's out of sync. And they usually gets reported by the very employees themselves that why is this lab and why you're here, why is this, you know, going on here. They look for overlays that where you have overlaps of information between people and they go to clean it up. And one thing I thought was rather interesting is, during system downtown periods or system upgrade periods, they actually intensify their search to try to find the possibility that somebody is taking advantage of the fact that the system is not, you know, fully operational or taking advantage of the business continuity efforts that are going on to steal information.

>>John Loonsk
So that's a potential opening in the system when the systems are offline and having access, or is it an opportunity to do more detection because the systems aren't being used for their primary purpose?

>>Harry Rhodes
What I found is that when you have a system downtime situation, especially if it's a nonscheduled one, you go to your business continuity plan, and a lot of times a

business continuity plan will cut corners and you're less diligent, and of course, you are compromised because here you are you got to use the system and it's taking a lot of your time to do it manually, and it's, you know, in the whole period, the whole chaotic period, for someone who's looking for an opportunity that that's the situation where everybody's busy, they're trying to do the operations manually. They're off guard, the systems not operating right, so they might not even notice that something isn't going the way it should. So, I think it's very wise to pay attention during those periods.

>>John Loonsk
Clearly, for detection, there is an issue of who can access the data in a way that they can be used for detection purposes, and we heard about payers, we've heard a little bit about providers, but providers don't always have the whole picture. And Debbie and Liesa, if you could talk a little bit about other opportunities maybe that HIEs can play.

>>Debbie Banik
As I was listening this morning, I was jotting down notes from our perspective, HIE perspective because we have one of the benefits of having a large amount of data from multiple data sources. And I started to research a little bit more when I was asked to participate this, and something occurred to me was we get real time information from our data providers, our subscribers, and with the course, you know, who has access to do this is an important part of this, but one of the things we could offer to them is to keep eye on things much like we do Indiana with the Public Health Emergency Surveillance System. There're indicators that this doesn't look quite right, or the red flag laws in the financial industry, something is coming in and that you've got a patient that has had this certain amount of care in this area of the State or we raise that to the National level of the country, and all of a sudden we're getting something else coming in that just doesn't make sense. And that, I don't think, from a technology standpoint would be that difficult to do. It's more of who has access to our data providers. Allow us to use their data in that manner. And then the next step would be who you contact. Do you contact the data provider saying you may have an issue here with the person that's in your facility that is not the person that has this in depth medical record? And again, we've got the benefit of having a lot of data in Indiana because that started being collected a number of years ago, so we have some transits to this patient has had this type of problems, and now you've got this whole off the wall type of problem, or you could start setting some benchmarks to what is that sets those red flags. And then the next step is who then do you contact.

>>Liesa Jenkins
Well, I think, what you hear about is how difficult it is to do the audit trails and how much time and sensitivities, and technologically, difficult to do them.
One organization that I'm aware of that has had some success in auditing is been doing what they call 120-day audits. In other words, what that is, 120 days

after the patient’s gone home, you should’ve finalized all the bills and everything else, and so they look from the discharge date, patient’s discharge date and they look for blips of activities that are beyond 120 days since the patient’s gone home. And they’ve had quite a lot of success in finding, you know, where someone, the patient, you know, he’s been gone for at least 120 days but someone is going into their records and they’ve been discharged and they haven’t been readmitted. So that’s a simple audit screen that you can do that has worked well with this organization.

__>>John Loonsk__
Can you talk a little bit more about, we’ve heard audit trails and audit, describe--maybe you could give a little more background on the types of audit being done in provider organizations and just what types of systems.

__>>Harry Rhodes__
The things that I’m aware of from--we’ve done a lot of research for articles at AHIMA and we’ve done some articles on audit trails, and this is because people very interested and also because they say that it’s very labor intensive and difficult to do. But as we talked about it earlier today, the likelihood that the person knows the other person who’s looking at their information at the facility on, you know, there’s a high percentage that that might occur. People do a lot of like names, searches, they do a lot of address searches looking for people that live on the same street, or they do zip code searches, and stuff like that because that’s a way for them to identify, you know, possible situation where people have access through the facility, either employees of the facility or, you know, they’re volunteers that they have access to the information of their friends and family. And since you hear about that there’re a percentage of people who the family willingly gives him their health information, their insurance information, and there’s a percentage of it that they didn’t realize that their uncle or brother had taken their information. For that population where, you know, a family member goes in or a friend goes in and takes information, then like name searches would help you and zip code searches and street searches would help you identify situations where people who may not have been looked--may not at a need to look at that record were looking at it.

__>>John Loonsk__
So there really are two very distinct detection issues: the systemic ones and the sort of one off’s that have been talked about.

__>>Debbie Banik__
And John, you asked about the role of an HIE in a weird, modest, naturist, the Indianapolis Health Information Exchange, but we’ve spent a lot of time with the folks and there is definitely differing levels between the hospitals. They have different situations to audit--really then, then ongoing ambulatory practice. And as difficult as it is to make sure that you have all the things in place for an individual organization, you’re just kind of magnifying that when you try to exchange

between organizations, like we're talking about what health information exchange. So, it does take a lot of work upfront to think about, you know, what kind of audits are going to be done--of everyone, what's reasonable to expect of every organization, and who gets to see that information because that's sensitive among competing organizations, multiple organizations sometimes.
I think that's going to be--we had quite a bit of discussion about what level of access should the patient have and does the provider need to be notified first if a patient requests an audit or a reporting of an audit. So, the health information exchange, I think, really what, at least what I have seen in our region, is it has very much heighten the awareness of the individual organizations that these measures have to be in place, and a consensus of what is the base level that everyone has to meet.

>>John Loonsk
Harry?

>>Harry Rhodes
I think what will probably help in your environment is to, wherever you're working, is to do an ongoing risk assessment, and not only just that you find out what's going, is that you share it and you have some sort of historical record.
Because based on your past experiences and your known weaknesses in your organization, then you can have a better idea of where you should be looking and that--instead of looking under every rock, if you have an ongoing risk assessment, then you can see where your weak areas are and you can see where the problems you have in the past, and you can be sure to go back to those areas to look for possible, you know, breaches in the present.

>>John Loonsk
So, I'd like to--we've talked a bit about, sort of, the systemic detection and some of the tools there. Maybe if we can go towards the one off's or the roles and which the solutions may be a little more elusive. And, I think, one potential tool in this regard is, is the PHR and the patient's access. And we've talked a little about patient's access to information and how that can potentially facilitate detection. And, Lory, maybe you could talk a little to that point.

>>Lory Wood
Sure. There're two issues here. One of which, once a patient begins to get their data connections to their clinical data and they begin receiving it, there's always questions about it. So, they typically call our helpdesk and want to know, most of the time they say there's a mistake, and we're, you know, we say, "Well, we hate to know that there's a mistake, but give us the details and we'll help you investigate it." And so, we assist them through the process; we go back to the source of the data. The majority of the time, we find that it's correct data.
There are some instances when there has been errors or has been mismatching. So far, we have not found any medical identity theft, but there's definitely the potential there. We also have open transparent audit trails of all the data, how it

was sourced in, and also, who has had access to their record all the way down to the record level and whether or not it was just viewed or if there was actual work done on the database. So, all of our systems are completely open for the patient to see who has had access and then be able to report back if they see any consistencies. We push out education to them, through emails and newsletters, encouraging them that if they found any kind of abnormal information there that they give us a call. We definitely encourage them to do that, and it's not one of those, you know, your problem, you know, your just you're on your own. We've got a great Customer Service Manager, and typically the things that are with wrong data get elevated up to his level, and he works with them one on one.

>>John Loonsk
Lisa.

>>Lisa Gallagher
I just wanted to add that I did give some information this morning about how…How well providers are doing at this point with providing patients, resources, to identify and report suspected medical identity theft. And that was only 25% of the organization, and those organizations that actually aid the patient in correcting the records was as low as 20.6%. And I think that the kind of open model that we see with some of the PHR vendors is something that maybe the provider should take a look at. We do see some cultural issues there where there's some resistance on the part of the providers, in particular, the clinical personnel to, you know, make changes into the record. As we've heard this morning from some of the folks on the panel early, there's, you know, some cases where they'll make a note or make an amendment, but if we have, you know, a process in place whereby we have a dialogue with the patients about their record in the provider in the organization, so that would go a long way to help with detection.

>>John Loonsk
One of the questions that were submitted was about this issue of giving patients access to records and really specifically ask about the pros and cons.
So, obviously, one con would be if the provider is less apt to put information into the record if he thinks or she thinks that that patient has access.
So, anyone else want to try to answer this question about the pros and cons of giving patients access?

>>Calvin Sneed
I know, from working with some of our providers, they, you know, there is sensitivity to how patients interpret the information in there if they don't have a clinical background. So, it's not so much an unwillingness to share that with the patient. It's just to make sure that there needs to be a context or someone who can explain what the information means, if the patient doesn't understand. What we're finding out is that, the providers who have been using our PHRs in there introduction into HIT, their patients are much more engaged, and especially

those that are chronically ill, they are on a regular basis going in and entering, you know, their blood glucose, you know, blood pressure, things like that. We also allow for secure messaging to the doctor. And they have found that it's improved their relationship.

>> John, one of the real issues that I hope is being resolved is when you talk about ways to access or ways to show the information to patients or audits or whatever. If every single clinical system does it a little bit differently, that's pretty confusing for the patients to compare the various formats in which they get stuff for the pieces of information. And so, the inoperability challenged around this is a pretty significant when I think--it's going to take awhile. I know the public's expectation was that we could turn this on tomorrow, but it's going to take a little while to work through this thing.

>>Lisa Gallagher
So, we may actually be talking about inoperability of auditing information and the issues at interfaces as well, which in detection, I mean, you know, quite frankly, these systems are designed to keep everybody else out that is not a part of their system, which is the total antithesis of inoperability and exchange among varying systems, not just providers, but PHR systems and clinical systems.
It's designed not to be inoperable in many instances. Another question on this was whether providers actually see their to-be liabilities for themselves in making their information available. And that's a big policy question. I don't know if anyone wants to talk about it, but it's certainly something that comes to mind.

>>Debbie Banik
Just to add, as I've gone around the state of Indiana trying to get more and more data sources to come onboard, that issue has come up from providers asking me, "If I have availability to this information, am I going to be liable if I don't look at it?" And that's somewhat of a concern to the physicians is, "Okay, now this is all available, what if I don't look at it? Am I going to be held liable for that?"
And so, having this information readily available at their fingertips causes some providers to be a little concerned about that. And I think it was Harry this morning who mentioned the fact that the electronic health record is considered by most, or any clinical record, is considered by most providers as a business record. So that's another reason why there's concern about, you know, looking at the record, and saying this information is not good, take it out, it's a record for the business entity itself. And that's an issue that we have to address as well.
>> I'd like to add that, I think that the value of data integrity, far out ways, the likelihood of any sort of litigation or anything, and I think it actually would help to prevent a lot of the situations where poor quality exists in that you have an extra set of eyes just looking at it and, you know, bringing it to your attention.
And I want to add what Lory had said that I think that--okay, I know we're focused on medical identity theft--but if the patient brings us something that's not right in their record, that we should walk on them and encourage them to come back and always point that out to us.

Because if we can improve the data integrity record, then we could solve a lot of quality issues that are out there that a lot of the things happened because the wrong information gets to the wrong person or it doesn't get to the right person. And so, I think that the value of data integrity is far out ways any other issues. I think it actually would probably, in the end, be a greater value than locking up the record tight and not letting anybody see it, not letting the patient see it.

>>John Loonsk
Calvin?

>>Calvin Sneed
Well, we've heard a lot today. The words were not quite there yet.
And, my primary physician recently notified me that he was going to be moving my paper files to electronic data files. And so, when I dropped off a form that they had asked me to fill out, I asked the women at the front desk if I would be able to access my records online, and she said she had no idea. So, it points out that, you know, we're not quite there yet, but I suspect that someday I will be able to pull out, log in to his account and pull out my record and do what we're talking about.

>>John Loonsk
So, let's move on to response now. And I certainly, as EHR have become more prominent, there are a lot of things that you can do to shut off data access when there is a response. We heard earlier today that that can be an issue, as much as anything else for the patient, in terms of bad access. But, Harry, could you give us a little bit of a background on what conventionally happens in a provider setting or other settings when something is suspected.

>>Harry Rhodes
Hopefully, you do already have an organized response in place and you have a response team. But often, the emails and phone calls that I get are the people who are in the middle of it and they don't have a response team and they don't know what they're going to do. And when we're doing our environmental scan, we were surprised to see the people who were named or responsible for responding were all over the place and there wasn't really any kind of consistency. It could be the compliance officer, it could be IT risk management, it could be AHIMA director, or, you know, social service nurse. It was interesting the people who were named. I do think that you need a plan to identify and stop the source of the leak or the breach immediately. You need to be able to identify the individuals when you take steps. To identify the individuals, you need to carry out a forensic for evidence. You need to be able to identify and sequester the record--and that's the subject of the identity theft breach. And, more than that, I think you need to go back and evaluate it. But what I usually find is that, and this is probably just because most of you went up calling us and we do have a good group of people that do call us and say, "I'm in the middle of it, and what do I do now?" And it was one of the reasons why--some of the first tools that we

created were response checklist. We created a response checklist for providers and we created a response checklist for consumers because we felt like at this point that would be really a value to--and just have a list of what I should do first and what I should do second. And we tried to encourage people to not wait until the day it occurs, to think ahead and have a plan and place, because time is of essence when it's happening.

>>John Loonsk
Other perspectives from HIE or PHR on round response?

>>Liesa Jenkins
Yeah, what you were describing, in one instance, in one organization, now, think about that shared among multiple organizations that may have all have to response and each of them have different plans and a different chain of command. So, the HIE definitely does complicate it. As CareSpark was going through, working through some of these issue, we were fortunate, but it was, it was, you know, I pulled my hair out sometimes in the discussions around the policies that everyone could agree to that this was a reasonable approach and we all should do this and that's what's in the data sharing agreements that we have. So, it definitely has required a rigor and I think has probably strengthened the internal policies and operations of each of these organizations to go through it collectively because they learn from each other, number one. But secondly, you know, they're holding us, the health information exchange, to a very high standard that sometimes they found that they themselves as an organization were not really living up to.

>>John Loonsk
Are there any other comments on response because we're getting a lot of questions here in the context of prevention and using HIT for prevention?
And I like to move to that if there are aren't any others. I think, what we're going to get to here is the questions about authentication methodologies, and different devices and whether if some of these things can be helpful. And so, maybe we can start at the consumer side, Lory, if you could talk about, sort of, the issues around PHR authentication and consumer authentication. Then, we can move to providers.

>>Lory Wood
Yeah, one of the, one of the biggest problems we had when we began offering our PHR doors subscribers is that in trying to receive the clinical information, if you're not a tethered PHR where you're with the payer or at EMR, they had fear of giving that information to us because they wanted to be--have a high level of assurance that that data was going in to the appropriate record. So, we came up with the process where, for identity proofing, when we began originally, it was a face-to-face identity proofing that was done through notaries. Now, we have a remote identity proofing that's actually used very stringent that is now beginning to be accepted within the market with PBMs and payers and things like that for

us to be able to receive data. But that's been the key from the PHR perspective is making sure that we have appropriately identified that person and it's not just someone going to a registration site filling in the information that they say that they are, who they are and then begin receiving data.

>>Lisa Gallagher
In our survey data of the providers, we did ask again about changes in business practices and improving patient authentication with the single highest impact area. So, we had 52.9% of the respondents said that they had improved upon their patient authentication methods directly in response to the threat of medical identity theft. My feeling is that that's probably, primarily, in the hospital organizations. And I think some panelist mentioned that this morning.
I think in the physician practice offices that's not something that is a wide spread practice at this point, you know, any rigorous authentication methods or identity proofing methods such as those that Lory mentioned.

>>Debbie Banik
So, even when the patient is authenticated, we still have patient identity issues that exist throughout the system and we certainly can talk about that at, a health information exchange level, but also at a provider level and would people like to elaborate a little on some of the challenges of and the implications in this area.
I knew from the health information exchange area it certainly would make our lives much easier if there were unique identifiers assigned to each provider and to each patient. And in the absence of that… And of course, I wasn't leading you to that answer. Yeah, and I'm not sure I would advocate for that but it's a reality that would be, it would be an easier solution if it were. So, in lieu of that are now some technical solutions that are pretty sophisticated for matching various aspects of information about either the patient or the provider not requiring social security numbers but, you know, algorithms to kind of do that and be pretty strong or at least tell you what level of accuracy you can expect out of that matching. So, I think you have to have that aspect as well as the authentication of the individual. But you, if you're matching multiple set of records for an individual that is a necessity you cannot do without that.
Yeah, I would agree from the HIE level. In Indiana as well, there's a patient matching algorithms that we use that are in-place. We often get asked about, "What are you going to do about a PHR?" And the patient authentication is one are that keeps us away from that is that we cannot be sure that the person logging in is the one who should be logging in. And so, you know, right now I think our direction on that is still currently to be, from the security level, not looking in to PHR, just that we--you just can't be sure. And until we've got that solved, then we probably won't move forward in that direction. But the data that comes in from the data sources and the patients, like Lisa said, "You have to have those very advanced algorithms that can match up information and with a level of specificity and sensitivity to be sure that who you're putting together is correct.

>>Shanda Brown

And along those lines we at Mass General hear so much about this issue that we formed a work group, it's a patient identity integrity work group, to bring the industry together and start talking about, first of all, defining the problem so that everyone understands, you know, sort of what we're talking about. But also, talking about the use technology and helping us do this kind of matching.
And we're at the very early stages. As I said, the first work product will be a white paper that describes the kinds of challenges that providers HIEs are having matching records as well as integrating PHR data as well. I should say, you know, being the recipient of lots of invitations from various vendors, to look at their solutions that the past year or so really, I have seen some emerging technologies that make me more comfortable with the ability to authenticate.
You know, there are a whole range of things that are, you know, token-based and remote two-factor authentication and lots of other things. And I think the combination of those two pieces is much stronger than it was even a couple of years ago.

>>John Loonsk

So, we talked about the patient and we talked about them authenticating.
We talked about identifying the patient and doing matching algorithm for this.
Where are we with the provider and all the identification of providers and access to systems? Harry, maybe you could comment on sort of where things stand in provider organizations?

>>Harry Rhodes

Well, from my experience, those common type of access management control is in for providers, is role-based access and that is effective up to a point.
Where I see downfalls with that is the due diligence to keep that up-to-date.
You really need a dedicated security administration staff because what happens is that people get promoted and a lot of times what they'll do and they go back into their access management profile and they'll give them new authorities without taking back--taking away their old authorities or it's the hassle factor, a whole lot about high hassle-factor of doing all these. And it's a whole lot easier just to give them, you know, greater access, you know, rather than trying to narrow it down and then you're out there depending on that person to behave themselves. You see things like, where people are under pressure in a big hurry and what sort of access should I give this employee and then you go, "Well, give them the same access as Mary over there," because you're a manager who's, and a lot of times from what I hear and from my experience it goes back to the supervisor to decide on the access manager profile who gets to do what.
And if that supervisor is uneducated or doesn't see the necessity of it, then, you can have people, you know, down falls in the system. Some of the other things that I see is when people leave a lot of times, I notice when someone is fired, they get walked up by security and they walk them up the front door and they turn off their access right away. But two things that I'm hearing about AHIMA from our members and from the industry as a whole is a lot of people leave under

pressure, right? And it's not always a good situation but so because they resigned and because no one wants to talk about the fact that why they resigned, you know, they don't walk around saying, they resigned or under pressure, that's usually kept very confidential, they don't bother to tell he IT department because now it's a different from, if you got fired, you're IT knows and you turn of their access right away. If you resign, you may or may not tell IT I hear IT people say things like, well, the only way we found out is when we saw the email about the going away party or we saw it on the bulletin board that the person was leaving and they didn't think about telling them. And now, when you have so much remote access by employees, the person doesn't even come in there.
They can dial it in. You know, they can, from their home, they can access, and if you aren't diligent in turning off the access when they're terminated for whatever reason, you have a real problem.

>>Debbie Banik
I'd add to that as well from the HIE side, one of our challenges when you have physicians that are in a community like ours, they can practice in a number of different hospital. And within that hospital, they can have a number of different ID's. And so, we have to be sure when we're delivering a clinical result that, you know, Dr. John Smith is this physician with this ID at this hospital and this department within the hospital. The other part of that is done manually, getting on the phone and calling, and saying, "We have Dr. Smith who practices at this hospital, is he still at this office? Is this still his fax number?" And we have to verbally verify that and then ask the physician offices to sign that, "Yes, these are the physicians. These are the users. These are the people that we want to have access and you'd be surprised at how many times the information that we will get, the provider has moved years ago. So, much of it is still a very manual process in conjunction with the technology once we verify it to match the physician up in the global provider ID area. And I will take that one-step further in looking at our health information exchange participating in the nationwide health information exchange. Let's say, even that, you know, it's a physician from a different organization that's requesting a record, okay, you probably still now who they are if it's a small enough community. But if this request comes from California or wherever, you know, then, you know, who is that person and how do I find out whether they're legit or not. You know, the reality is right now, you get that request by fax sheet, probably, you fax it back, and you don't bother to check. But, somehow, there is a fear factor that comes with that coming electronically. And one of our providers even asked if it would possible to be notified every time someone requested a record on his patient. Some of the other doctors look at him, like, "Are you crazy? I don't want to know every time looks at one of my patient's record." But he did. And, you know, so, I think that, again, that magnification of the complexity is the reality for health information exchange and the challenge for the nationwide health information exchange.
One of the questions we got was about roles HIE may play in communicating alerts or either to provider or to patients and whether that's an opportunity or…

Well, I know that in the context of that discussion one of the questions that was asked of us was can you do the credentialing, that way, we know, you know, that from another organization or whatever that they've at least been verified by CareSpark or somebody and we don't have to worry about it that way.
So, that is a role, not that CareSpark has chosen to do that yet, but it is a role that an HIE can play and some may choose to do that.

>>Lory Wood
And I would agree with that and as, you can tell when you've got one HIE, you've got one HIE. But the, I think, that's a very valuable benefit that an HIE can provide to the community that they serve is that notification and alerts especially if you've already got some sort of delivery mechanism that your HIE has put in place out to the physician community. It would be a fairly simple thing using that technology to provide those alerts to those physicians that your patient's information has been requested by so and so. So, again, and whether we choose to do that or begin to look at offering that as a service and whether your data sources wants you to do that is what the HIE can look at, but…
I know some PHR and some HIEs have a particular role for vulnerable populations and one of the questions is about whether there's an opportunity either in the sector or others to particularly look at vulnerable populations like the elderly and tools for monitoring that. And I don't know, Lory, do you have thoughts on that or…? Well, we do have several of the older population that is subscribers to the PHR. And again, it has allowed them to have a better relationship with their doctor. It also allows, we allow for proxies so we have several subscribers who have proxies through their children being able to log in to their account and look at it, monitor it. If they don't like the direction of the lab results and that type of thing that they can pick up the phone call a doctor and try to check up on them. But it is a connection that, you know, allows for those proxies to have value. I do agree that the elderly are most likely to be victims and, but all you can really do is reach out to them and try to educate them about how system works and what they can do to protect themselves and so they can better understand it. And if you, when you're enrolling them, if you realize that they do need a proxy, I think you should be proactive in offering that option and then, and making sure that someone besides the elderly consumers, the one who makes the decisions. So let's talk a little bit more about education since you brought it up and communication with others and whether it would be EOBs and how can we, how can the technologies help communicate things to patients in a way that they can understand and to others. Okay. Well, certainly, I think that as I mentioned earlier in the day, I do think that you could, a way of communicating with your patient consumers via email and you should have a way for them to be proactive and a way for them to reach out to you and actually encouraging them to reach out to you. And even if it's something that, that they may think it's trivial, you don't know that at the time and that I don't think you should belittling them or anything. I think you should have a welcoming, open environment, an easy way for them to understand how they can communicate. I also think you need to not think in terms of the average consumer. I think that you need to have more than

one option. I mean, obvious, not just an email alert. Not--maybe, a phone call, maybe a hotline or another way for them to communicate. And I do think that reaching out to them one on one and maybe, identifying somebody who's their advocate at the facility that they know and they feel comfortable with and they can talk to on a first name basis is a good way to go as well. You know, it's not just a cold email; you know that may or may not appeal to a certain populations. We do send out email modifications when data has been received into their record and asking them to review it. We also, not as much so anymore, but when we first began our program, we had several that would be covering different subjects and we'd send the invite out to our subscriber population to allow them to participate in that, which was also an open interactive session where they could ask questions, get answers. And it also helps drive the subjects that we knew that we needed to cover. I'm going to talk about a vulnerable population that's really not at that level, which is, probably, a lot of the folks in my community who are very low literacy, not just passive health care consumers but in general have difficulty navigating through systems and certainly technical systems. So, CareSpark has for a couple of years now, really been working with, sort of, seminars; we attend to health fares and Rotary Club meetings and, you name it, to kind of explain to people what it is we're trying to do and the benefit that we perceive. But we do acknowledge the risk that's there and responsibility that the individual has. You know not only the rights but the responsibilities that you have to protect your information. We've developed, as one of the tools just a very questionnaire that we pass out, you know, asking people, "Would you be willing to share your information electronically, and if so, with whom? And what kind of information would share, and what ought to be the penalties if it's released without your permission and where do you want to give your permission? So, really, starting at a very basic level to educate the consumers and the community using all mechanisms; we have information on our website. We have print brochures but for some people, you know, that is also not accessible information for them. And I had worked with a group of people were part of a billing organization and even those folks who are well educated and trying to understand the insurance industry when you see one EOB, you know, good luck figuring what it says even if you're educated in it. I think there are some real benefits for standardization across the insurance industry with standardizing what those EOB says and make them in plain English. Don't give the code that went in. That means nothing to me as a patient and very little sometimes to the billing people. So, there's a great deal that can be done on the information that comes back to us as patients to even begin to know if our identity may have been compromised. And I will second that thinking specifically about the audit logs and reports; namely, yes, patients have the right to know who has viewed their information, but how is it that that information is presented to a patient. You certainly can't do a print off from an audit log and make any sense out of it whatsoever. I haven't yet seen really simple tools for consumers to look at in that regard. So, if somebody has one, let me know.

I think the emphasis in this discussion about involving the consumer and the patient is particularly one that provider should pay attention to because what I see with regard to detection of these kinds of things in organizations is that we, they're pretty good at detecting, you know, breaches. They're not so good at relating it to medical identity theft and the bottom line is that right now, the cases that we do connect to medical identity theft are brought to us, by and large, by the patient themselves. And as much as we have all these fraud detection activities, and we know how much it cost to provider organizations, they really don't have a whole lot of choice but to involve the patient in some way in validating the integrity of the data that's in their record. And so, we do hear with the HIE and the PHR vendor see some models for that. I think the HIE themselves as they pull in provider organizations are going to be able to help them with that, outreach and provide models for that kind of outreach and start to see the value of involving them and perhaps even facilitate some amount of culture change in this area. There's one theme in the questions that has come up that we really haven't touched on which is, in the context of detection we talked about how important it is to access data, that aggregate a data can help in detection. The converse of that is in the context of prevention. What are the best practices to not aggregate data, to potentially separate demographics data from clinical data? There are questions about the new; the many companies that are now in the PHR world and whether they're aggregations of data will pose new risks in this regard.

>>John Loonsk
Can anyone speak to some of the best practices around storing data that help with prevention?

>>Lory Wood
Well, definitely going back to the advice about minimum necessary based on the job role that when you're setting up access controls that you should ensure that the person only has the information--has access to the information that they need to perform their job. And it's an ongoing thing. You have to constantly go back and look at the person's new job role and has her job role changed and are they accessing too much information? You can limit some of that information.
You can definitely, for your information, it's extremely sensitive, and you can definitely implement encryption practices that will encrypt the data and further control access to sensitive data. And, you know, just being aware that the person shouldn't have access to every piece of information, what do they really need to do their job. In PHR we have a whole section where they do authorizations on the programs that they're willing to participate in and they have the ability to revoke that at any point in time. But if their PHR is actually paid for by their employer, we assure them of the fact that even if there is an aggregate report that's done, it's completely identified. We also look at if it's a small enough employer that there's only two women there or something along those lines, they're not allowed to get aggregate reporting. So, at least not determined by sex, you know, in that instance. So, we have certain rules and policies that are in place right now, but the key is, is that the consents and authorizations are opt in, not opt out. One thing I just thought about while I'm sitting here. Another thing

you can do is when you're setting up descriptions and job responsibilities, if you have an individual who has control of a process from beginning to end, for example, they process the claim or they process the remittance and they're also the ones that can create accounts, you really need to have, in their job descriptions, you need to have separations of authority or separations of duty that this person doesn't have the ability to submit a claim, get a check back, and create an account or send the account to somewhere else. You should divide up those duties. There should have somebody with oversight authority watching what they're doing, but you do see a lot of that kind of situation where the person has control of the process from A to B to Z and no one else is watching them or even coming around the look to see what they're doing. From an exchange side John, you know, one of the things CareSpark's team talked about very, very early that's a little bit unique, I've not heard other health information exchanges do is kind of having checks on both sides of the conduit, if you will. So, in our system, the provider organization actually either releases or doesn't release the record based on what the patient directs them to do. But we have centrally stored one of the pieces we do have centrally stored along with the demographic information for that patient is a yes or a no. Yes, they want that provider to send information. No, they don't. And so, even if something inadvertently does get sent by that provider organization to us, if our system says no, we're not supposed to have anything for that patient from that provider, our system rejects it and doesn't accept it. And I think that, you know, that's just an extra little step in the process that maybe helpful. We're going to need to wrap up shortly, but as a final question to the group, do see any technologies that could be either helpful or could contribute to this problem and specific technologies that were referenced by the audience included Smartcard technologies for authentication, biometrics and the issues, the stigma plus the possibilities for biometrics and the advent of all kinds of new devices like wireless and handheld devices and whether those might contribute or help with some of these, of these problems. I don't want to look in to the future in their crystal does says we're wrapping up. The Smartcard and biometrics seem to be one of the solutions and it's surprising that it hasn't caught on, excuse me, it hasn't gotten much momentum as we would have thought. I supposed the privacy thing and the national identity card aspects are pushing that away. But, if, you know, if you have a card with all kinds of information that could save your life possibly, prevent identity theft, have your finger print on it, and be authenticated at the providers office visit.
It seems to me, you know, sort of the logical next step I think, a lot of people think it is the solution to a part of this problem. I think your--you know, the answer to your questions is yes to both. I think technology can be a huge help but the bad guys out there will find out ways to use it to help them as well. So, I think you're always going to have the really good sides of it and you're going to have the really bad sides of it. I agree to Debbie's point and I think we've heard a lot of examples of today of how really most of the problem lies in our business practices. And so, I always emphasize with the folks that I work with that, you know, doing on going risk assessment and understanding based on your business model where your risk are, doing privacy impact analysis.

You know, where is the data flowing and what are the privacy impact?
Those are the activities that will hold you in the best stead in the long term.
And then, you can determine from that analysis where to place technologies that will aid the process. But in the absence of ongoing risk analysis and in that sort of type of practice where the organization is taking a comprehensive look at their security practices as well as the privacy impacts that they face, then the technology is really not going to solve the problem. Where it might solve part of the problem and you don't recognize the problem elsewhere.
So, I think in context, it's very, very beneficial but the organizations really need to have an awareness and sound practices in place. And I think the technologies will continue to evolve but the reality is this, that there will be people who do not wish to use those technologies, patients, I'm thinking about primarily but also providers. And so, the burden will be for organizations that have to continue to have two processes, one that's technology-enabled and one that's not.
Technology is always an enabler. So, keeping that in mind, using a biometric may save the life of an unconscious patient and break the glass situation. There are several benefits to using biometrics and I think part of the thing--the methods that we need to be doing is educating people so that the, there isn't such a great fear factor about the biometrics. We do use digital certificates for two-factor authentication and we're now on implementing roaming certificates. They use voice biometric. We don't even turn on the Smartcard or the token until they have authenticated with their voice biometric. So, there are positive ways for these types of technologies to be used and I think we've got to educate the public so that they're not afraid of it. Well, definitely, I think that there's a real value to Smartcards, Smartcard tokens and one of the technologies I really am interested in and I've seen a little bit about lately is, proximity access where you actually, in your name badge or something, there's a device that, as you come near your terminal, your terminal turns off and when you walk away from it, your terminal turns off and I think that's--it turns on and off, sorry. And, anyway, I think that's all great but I think that going in to that, you have to realize that you are taking out a whole lot of other responsibilities that, if you don't have the proper administration and the proper security with these new technologies that you will have problems with token cards and with biometrics and you may just be creating a situation where you now have all the information in one location and the person who is committing the crime just do a one stop shop and get it, all your information at once. So, you do need to go in to that with your eyes open that you need to protect the administrative part of it as well. And then, it isn't without challenges. All you have to do is look at how Germany and--Austria has just started but they're still facing a lot of challenges administratively to get their Smartcard program going. And in Germany, these face a lot of problem in that, as you were saying, not everybody wants to go the same way you're going and they have a lot of competing initiatives and stuff and you have to realize that, unless you do a really great marketing job and win everybody over, you'll always going to have people who have a different opinion and will want to do it slightly differently and that will add to the challenge. And John, I would like to just make one more comment there. Security is obviously very, very important and

everybody is really concerned about it. I want to be assured to that, it is not so locked down that the people who need the information, take care of a patient cannot get it when they need to. And I haven't yet been really assured that that's not going to happen. And in that case, that just leaves those who are already frail, sick, whatever vulnerable even farther behind, even more at risk than they are now.

>>John Loonsk

I think we've teased out a number of those points about access and prevention and control, but, thank you panel for a very interesting discussion and let's give them a round of applause. We are not taking a break, the next panel will resume at 2:45.

Panel 4: The Path Forward

>>Morris Landau

As we talked about earlier, the purpose of this town hall is to talk about the Health IT and medical identity theft and use of Health IT in the prevention, detection and remediation of the issue. And, you know, as I was listening to today's panels, I was thinking that we have sort of developed, or at least I have developed a nomenclature and some themes. And the reason I'm going to sort of go through this quick laundry list of new words that I learned as well as new themes is sort of just to trigger some thoughts people in the web and also people here to think of questions as we move to the next half forward. So these are the new words I've sort of learned today or at least some thoughts, insider, one-off, access or right to access or appropriate access, that the system is easy to enter as far as claims are concerned, the consumers are not sure where to report, where to go. I've heard the word "gaps" quite a bit and loss in the health care system and quantification of the issue. Security breaches and notification loss, notion of stovepipes, that we need to get out of our stovepipes, red flags, audit trails, risk assessment, health IT to prevent that threat. Clinical cultural change, I thought that was interesting. Changes in the record that constantly became a theme. Liability issues, if you received the data. And, of course, on the Health IT side, we heard a lot about patient authentication and matching, proxies, education, explanation of benefits or EOB's. And, of course, we heard about Health IT as far as biometrics, smart cards, hand-held devices, and etcetera. So, that's sort of the continuing words that I'm constantly trying to keep up with as we're dealing with this issue. So, overall, the format is that Denise and I will meet in just a minute, we're going to just swap questions from the audience that we've got on note cards to sort of let the panel just have a free for all discussion, if that works with everybody. And please don't be shy and jump in. And so with that, the ultimate goal was to try to get people involved. How do we get people involved in this issue? And that means for the entire, not just the federal government, not just from the private sector, but also consumers, everyone in the health care system involved in this issue. So, with that, I'm going to let each person introduce themselves, and then Denise is going to take the microphone.

>>Denise Tauriello
Hi. Denise Tauriello based in Rockville, Maryland with Booz Allen Hamilton and I've been working closely with ONC on this project.

>>Harry Rhodes
Good afternoon.
Harry Rhodes with the American Health Information Management Association. I'm the Director of Practice Leadership.

>>Lisa Gallagher
Lisa Gallagher, Senior Director of Privacy and Security at HIMSS.

>>Betsy Broder
Betsy Broder, Federal Trade Commission.
And I'm going to, you know--we have our last of the presidential debates tonight so I'm going to do my little moment before you answer and say thank you to HHS ONC, to Jodi and to Morris, for showing the leadership that you have here putting together such incredible panels of experts from all areas. I think this really moves the ball forward so I salute you and I thank you for this event.

>>Leisa Jenkins
Leisa Jenkins, Executive Director of Care Spark which is originally Health Information Exchange.

>>Shanda Brown
Shanda Brown from Massachusetts General Hospital. I'm in HRS Department and our department is responsible for handling issues of medical identity theft and data integrity.

>>Pam Dixon
Pam Dixon, World Privacy Forum.
We're a public interest research group and we've done a lot of work in this area.

>>Denise Tauriello
Okay. Thank you, everyone.
I think we have heard a lot today about community and the victim and the vulnerable populations. And I think one of the things we want to want to start with today with the panel is how can we, as a community help victims, health vulnerable populations begin to think about dealing with this issue? Anyone in particular like to lead off? Pam?

>>Pam Dixon

Oh. All right. I just--a lot of thoughts are swirling in my head.
Okay, you asked. Thank you. I'll try to be concise. There are a couple of things that came up that I just like to respond to. This is a responder panel after all.
So, I just want to say again about authentication. Authentication is important, but it is a Pandora's Box and we have to be really careful of what happens with authentication. We had a victim who someone presented at an emergency room with an ID with her name and all of her information which was correct; and the hospital, the provider in this case, hardened that ID to a biometric that belonged to actually criminal. So, when the actual victim tried to prove it was her, she became the criminal. So we've got to be really careful of biometrics. It's not that, you know, some doom and gloom descends upon us because we're even thinking about using biometrics. No, that is not the problem. The problem is that they can be hardened to the wrong person, and criminals are very good at doing this, and we've got to really keep in mind the lessons we've learned from the DOJ on that matter. So, you know, what I'm saying is not that biometrics is some form of new evil. What I'm saying is that biometrics present enormous challenges in the use in a hospital care setting. The second thing that I would really respond to from today is that there, you know, Health Information Exchange brings a lot of benefit but it also brings greatly increased data stewardship in transparency responsibilities. And one of those responsibilities really comes down to what happens in the case of medical identity theft. When we asked, you know, what are you doing about medical identity theft, one of the things that we often hear back is, "Oh, we're thinking about it," etcetera, etcetera. And what we really want to hear is, "Well, we've got a process in place so when a victim comes to us, we can get the records corrected, or we can disseminate the information to all the different folks who have the data, or we can tell the victim where their data is so they can go corrected." But basically, I want to hear that there's a process in place for the victim, and this process, unfortunately, can involve multiple HIEs.
It can involve multiple states and something that I keep saying over and over again, we've really got to have a national level process so that there's some continuity for victims. And there are a lot of other things that I can say, but I think I'll try to shoehorn it in into other comments so other people have a chance.

>>Denise Tauriello

Thank you very much, Pam. Shanda, I know that you guys have been doing a lot of work in Massachusetts in this area. Can you highlight a little bit what you think is working, what's not working; there might be a benefit that we could deploy elsewhere.

>>Shanda Brown

Well, I'd be glad to, and I kind of liked the way that Pam segwayed right into this with the word "process" because I think that's very important.
And that's pretty much been key for the way we've been able to handle this was we've put in a response plan so that we do have a process in place.

And it’s important for several reasons, one of which is it does give the patient an advocate in a way inside the hospital who can handle the investigation and who can work with them and be a face and a voice to provide them some feedback as to where we are and what we’re going and what’s going on with that. You know, also, educating staff, raising awareness of the issue, and this is a great way to start this. There are a lot of people I know who are not here and also out in the web, raising awareness and, you know, how to identify red flags, just awareness of the issue in general so when they see something that in the past they might have just let go, in the past, they might have, you know, brushed to the side, “Oh, that’s kind of strange”; now, they’re thinking, “Maybe I should report that.” And that needs to be done both on the front end and the registration side and on the back end, the financial side. And then creating a way for once that awareness has been raised for both clinicians and non-clinical staff to be able to report any instances or even suspect instances to the right people so they can investigate it. So, we’ve created, in our case, the generic in-house email inbox so people can send a message to our patient index staff to kind of say, “I saw this in the chart, it’s really unusual, can you guys take a look at it?” So we can just make sure it’s not just the information got printed incorrectly, but it’s not a thread that we can then pull to make sure there’s not something going on there. So, you know, I think that a lot of the solution from a provider side is to really just have a plan so when something does happen there’s a way that you have to address it and that plan does need to include some communication to the patient so that they feel like they are a part of this process and they feel like they have a voice in this process.

>>Denise Tauriello
Thank you very much, Shanda.
So, we’ve heard about education and awareness and we’ve heard about process. Before we go on to another question, I’d like to at least reach to you Betsy and see from an FTC perspective what your thoughts are.

>>Betsy Broder
I guess we build on what each other is saying.
So, I heard a couple of things so far and first is one that, I guess, comes under the cultural rubric and I suppose what’s going on at Massachusetts General which is that from the top down, there is a message that security and privacy is everybody’s business. So, whether it’s at the registration, whether it’s at the treatment phase, that everyone is aware of a problem and that there is a program, a process for them to follow, that there’s not an ad hoc approach to this sort of problem. But something that we’ve sort of played around with as we tried to find the right framework in which to address this and something that keeps occurring to me is that we have two, at least, two, if not many more different types of systems and one is a close system. So, at Massachusetts General they can be aware of anomalies within their own data as to multiple uses of Social Security numbers and aberrations in terms of treatment protocol that suggests that there could be a problem. But from a federal perspective, we’re concerned

about this in an open system. So, when that person uses, you know, someone goes to Massachusetts General and uses information that otherwise was used at some other hospital system that is not associated with Massachusetts General, what are the protocol, what is the system for detecting the problem there. So, that's something that I think we still have--we haven't found that sweet spot. And then the third issue has to do, again, with notifying people whose information has been misused. In the credit context, we feel fairly secure that when someone contacts us and says someone has opened up accounts in our name, we can say contact the credit reporting agencies, report to the FTC, report to the local--I mean there's a whole protocol and then there's a whole set of rights that they have, that they can exercise and rights to which they are entitled. There's some debate, at least, at the very least, what the right protocol is, what the right remedies, available remedies are for victims of medical identity theft where there could be corruption of their file. And again, we have that same problem in a close system. If you're talking about someone who has misappropriated someone's health insurance benefits, it's a close system. You can see what the treatment has been and, hopefully, you're going to be able to address it because you're going to be able to identify the providers, but when you're talking about the whole ocean of providers, how do you address that? So, again, close system-open system, I think there are so many issues here for us to address and it's a challenging one.

>>Morris Landau
Thank you very much, Betsy. The one other piece of the people equation that I wanted to explore before we go on is that--which we heard a lot about, inside job, you know, that a lot of medical identity occurs inside an organization.
How can we tackle that people side of the equation? In other words, is it training and awareness? Is it background checks? You know, what are your thoughts about how to manage that side of things? I'll leave that open to anyone who wants to jump in.

>>Pam Dixon
Well, I would just say that AHIMA and HIMSS and organizations like that who already have developed some training for their professionals are probably the first place I would think to start to go to encourage the local folks in our community to be aware and know what to do and what kind of the best practices are. I think those are great organizations for disseminating information about some of the issues and then as solutions are forming to share them. I think that one of the things that--I really appreciate--is Harry still here? I really appreciate a lot of what he said, you know.

>>Denise Tauriello
He's here, way down here at the other end of the table.

>>Pam Dixon
Oh, there you are.

I really appreciate a lot of the things he said in the last panel. I'd like to add on top of what he said in the last panel. And, you know, when you talk to the DOJ and the FBI and the health insurance investigators, the people who are in the trenches of this crime, what they will tell you is that it's--role-based access is great. But a lot of the times, crime are committed by people who have legitimate access and they have used their legitimate access legitimately, in other words, they're doctors or nurses. And an employment background check may pick some of this up, but going back to the very first panel with what was said which was if you have a determined criminal, they're going to get in. And I think that what we're seeing here is the rise of the determined criminal in this sector. And it's not new. This is health care fraud, but a new twist. But the problem here is that there's this--and I don't mean this in pejorative way at all, but there's a certain almost innocence among health care providers where you have so many good apples in the barrel who are really there to help other people. You really see people who are helpful people, people who really believe the best about other human beings and then there are just really awful people who are doing these dastardly things that are just--I don't know. It's just remarkable how awful they are. And it's almost as if the actual system doesn't want to believe that they exist. I think we need to believe that they exist and I think that we need to look at the people--role-based access is great, but look at the people who have legitimate access. And I think when we really start to look at this problem and how to solve it; you have to look at the people with legitimate access, not just people who are abusing their role-based access. And these are very hard criminals to catch, but I think that's the task.

<u>>>Lisa Gallagher</u>

Yes. I'd like to add on to what Pam said. You know, it's funny for me because I have a technical background and I did, you know, information security audits for 20 years and I focused a lot on technology, but I have to say that in most of the audits that I've done, you know, the issues, the weaknesses are really with the people and the processes. And, you know, in health care organizations and we've talked a little bit about the culture in provider organizations, they are caregivers, there's a care environment there, information by and large is shared for the benefit of the patient, to take care of the patient. And so, when we talk about how to train those personnel in data security, you know, I like to say, tell them that part of taking care of the patient is taking care of their data.
Care of their data is, you know, part of the overall picture for the patient.
And when you explain it to them in that context, they don't think about it as a burden, as a, you know, extra requirement that's placed on them, but they know that they've got a patient there in front of them and that their data is just as important as their health in the long term. I think with regard to the organization itself, you have to do audits of employee practices. So, you're going to have policies in place and you can have training, but unless you know what they're actually doing on a day to day basis, you're not going to find the places where you're vulnerable. Also, you can rely quite a bit on the good apples, the people

in the environment to start to look around them and see things that don't look right and report them and put, you know, a process in place where that's a positive, you know, patient-supportive thing to do. And so, again, it comes back to the cultural issues in the provider organization and the supporting practices of the organization.

>>Morris Landau
I think that's helpful and I sort of want to push the envelope a little more than this, which I think is a good thing. What I've heard is we have a close system, we have an open system, what processes--we need to put processes in place. So, I have sort of a two-part question to this. One is what can we learn from other industries. What can we gain from other industries that we can hopefully apply to the health care system? Part two of that question really deals with what should the processes look like knowing the scalability and the flexibility of small physician practices, large hospital systems, health information exchanges. We talked about processes, but give me some more specificity of what it should or what it should look like. So, first of all, dealing with other industries, what can we learn from other industries? And whoever wants to tackle, tackle that.

>>Pam Dixon
With regard to the financial industry, I think there are two things I'd like to note. One is that the financial industry, in particular, credit card vendors, at some point came together and decided that they needed to deal with the threats that they are facing together as an industry. And so, they do share data on threats and they share data on vulnerabilities and they work on these problems together. And together, the major credit card companies came up with the PCI data security standard, the payment card industry data security standard and they hold their credit card merchants to a certain performance standard with regard to security and they audit against that. And that's not a regulation. That's not a law. That is a requirement that is generated within the industry to bring the level of practice up to, you know, a best practice level. I think that the dialogue and the sharing around the threats and the vulnerability is a place to start and then finding common mechanisms to enable everyone in the industry to bring security and privacy practices to a certain level. It's sort of a model, not that you have to do it exactly the same way, but we don't tend to share this kind of information right now. And I think, you know, what we're doing here today, talking in general about the medical identity theft threat and to maybe even talk about as the next step some level of information sharing so we can start to understand the sources and the motivations of those threats and institutionalize our reactions to those.

>>Betsy Broder
I would add a little referring to this that in some, it's interesting to talk about the financial or even the credit card industry because, of course, there was a time when the credit card industry was rife with fraud, but there were no sufficient internal incentives for credit card companies to do anything about it. And so,

Congress passed laws limiting consumer's liability for fraudulent uses of credit card numbers. As I recall, the credit card industry was not at all enthusiastic about that. But at the end of the day, they realized, it made consumers much more comfortable using their credit cards, and in fact, encouraged--expanded on acceptance of that. And so one thing to look at, and I guess this is the point at which I put in the disclaimer that anything I say reflects my beliefs only and not necessarily those of the Federal Trade Commission, is that there are an internal incentives and there are external incentives and both have to be evaluated.
And to a certain extent, health care providers, insurance, others in the payment stream have an incentive to do the right thing to take care of their patients and I don't minimize that. And I think that voluntary programs to create standards, interoperability, resources for consumers are fabulous. And perhaps, that can be sufficient. But at times, those incentives are not sufficient and that's the point at which I say I was speaking on my behalf only. But, you know, I think we're at the beginning of the dialogue here and on the cusp of a very different health care environment. And now is the time to have these kinds of discussion or else you see how it plays out and you see what needs to be fixed.
It's another way to look at it.

>>Harry Rhodes

I'd like to say that I do think there's some value to the notion of community.
All of us that have sat in these panels today, we all are shareholders in the same problem and we have a common interest and I think that there ought to be a way for us to have a clearing house where we can share what works. And I'm really interested in communicating to actually our members what works, what doesn't work, what's your level of commitment, how much is it going to cost you in time and money, and, you know, to give them the power to make better decisions.
And I'd like see us; you know, form a community, form a face book for all of us so that we could get together and share some of these ideas. And I've actually learned quite a lot today about things that hadn't even occurred to me even though I've spending a lot of time researching this and there's a real value from that. And I do think that there's a wave of change that can occur through a community of stakeholders.

>>Liesa Jenkins

Morris, you asked the question about other industries.
I actually think that law enforcement and the military are probably an industry from which there are some practices that we could learn from. You know, they have people who have access to different levels of information. They have to respond to crisis situations and they do tabletop exercises. I would, you know, in addition to a face book--maybe it's a good thing actually. I thought about this for our Health Information Exchange of doing a tabletop exercise, if you will, with the participants in the exchange to simulate a breach and, you know, what would happen. I think that's a good thing to go through. That may be part of the risk management planning and response development.

>>Denise Tauriello
Other thoughts, Pam?

>>Pam Dixon
Yeah. I think some of the big lessons are, first off, transparency does work and it does build consumer trust, and at some point all the health information exchanges and regional networks, etcetera, etcetera. Although this is going to be surfaced to the consumer, that consumer is going to have questions and needs to have transparency to help get those questions answered appropriately. So, I think transparency is a very important model. I think also another thing that works is the model of anything that's had something built in from the beginning as opposed to baked on at the end. So, an example of this are some of the very deep level like HL7, etcetera, structures within the health care sector. One of the things that I really see at this point is that, you know, when we go into our providers and we've done an awful lot of that in the last half year, we've toured a lot of providers and we say, okay, so let's say that this record--this patient, you know, comes to you and says, "I'm a victim of medical identity theft, show me in your system right here right now what you can do to mitigate that."
And most of them say, "You know what, our system isn't designed to do that and we would just simply have to delete the record or they'll give me some other workaround and as many providers as I visited, that's about how many workarounds I've seen. So, I think that building in from this point forward, a thinking process and an architecture regarding mitigation of not just medical identity theft, but health care fraud in general and its impacts I think is something that's going to need to be done. I think that there is such a push to get Health IT going that it was a positive effort and not a lot of thought was given to the downside. And I think we've really got to, at this point, turn to the downside and say, "Okay, let's mitigate for the problems that we know that we have."

>>Pam Dixon
I've had the experience, Pam, of being involved in a number of implementations and it's amazing when you're doing the implementation, you're thinking about all of the bells and whistles and all the benefits you're going to get.
But I've heard a lot of sage advice over the years and one of them is that you should start with security administration before you even look at the first product and what do you need to do to rule out this application and to implement it and to protect the security of it first before you even start to buy all the fancy things that you wanted to do, and I do really think that that's important. And then the issue about--I had some discussions through networking sessions with our members who have employee sanction processes, but because they're not sure because they don't have a clear model to follow, they suspect somebody is stealing information, but they don't act because at what point do I act or what's the process or when do I have enough information, when is it going to be ironclad and the whole time that they're waiting around for a signal, the person is, you know, actively committing a crime.

>>Denise Tauriello
Thank you very much, Harry.
We're going to switch gears just a little bit and talk about technology.
We've had a nice lead-in around health information technology.
I have a question from the audience that kind of gets to the technology question and it is we have lots of data, what data-mining strategies might have value in detecting MIT, Medical Identity Theft? Liesa, would you like to start off?

>>Liesa Jenkins
You noted my disclaimer which is I am not the best technical person on my team, but what I can say is that it is very important that you have business intelligence tools kind of constantly monitoring. I think that counts as data mining. Maybe, it's just kind of watching the flow of stuff that's going through and sensing, if you will, or recognizing some of the patterns for things that are out of whack and then being able to look at those. So, you know, I do think there is an ability to compare what would be expected and what's not expected and then have a way to analyze that.

>>Morris Landau
That's good. Well, Lisa Gallagher will come in behind you and dig a little deeper.

>>Lisa Gallagher
I was going to focus a little bit on the security side. You know, I've worked in a number of different industries. And traditionally, security is described with three components: confidentiality, integrity and availability. And I've noticed that in health care, we primarily focus on the confidentiality aspect, but I think that the integrity aspect is something that the security folks need to help us in the provider organizations to understand and put into its proper context with regard to the work that we do around security and health care. There are a number of technical techniques that have to do with just the pure data integrity and the records and looking at modifications, alterations, and integrity as data is transmitted. That can--perhaps, it's not a one-stop solution, but it is part of the equation and so I think we need to broaden our focus beyond just the confidentiality aspect and really focus a little bit more on the data especially when we face these kinds of threats.

>>Pam Dixon
I agree with Lisa.

>>Morris Landau
And one of the things that we heard--I'm sorry.
I'm just going to pitch one second, Pam.

>>Pam Dixon
Yeah,--oh, go ahead.

>>Morris Landau
I just want to--the other thing that we heard in our research around this issue was around things like pattern recognition technologies. Has anyone heard anything about that? Is it being used? Are you aware of it being utilized in the health industry?

>>Betsy Broder
It's certainly is being used in the financial sector. Neural networks to detect anomalous conduct. And one of the earlier panels, they talked about procedures being done on holidays. It just seems like not right. These are red flags, you know, things that don't necessarily say that this is fraudulent, but requires some greater scrutiny. But I guess being as far from a technologist as anyone on this panel, what I would say is that what might be the right technological approach one day may be obsolete the next so it also must be dynamic and assessed as part of the general risk assessment, whatever technology you embrace to make sure that it deals well with the risk that you're confronted with as we heard on the first panel. From DOJ the more sophisticated fraudsters will find, you know, the vulnerabilities that are least likely to be detected and they will work them and work them until suddenly they're detected. And then, you know, you need to be able to then compensate. You know, you found the vulnerability, what comes close to that other vulnerabilities so maybe you can step a little bit ahead of the bad guys.

>>Morris Landau
Great. Thanks. Pam, go ahead.

>>Pam Dixon
I want to follow up on the data-mining question. It's actually a really interesting question and it gets to Betsy's inside, or not inside, but, you know, closed-open system issue. That's actually a very significant issue because you can data-mine your own silo but you can't data-mine the whole world unless you're Google. Sorry, that was a joke. And, you know, one of the things is that, you know, one of the things we really see in health care fraud in terms of medical identity theft is to really fix the problem, you can't data-mine in a way. You've got to involve the patient at some level because, you know, they live there, they live in that body, and they know what health care they received. And at this point because of the fractured system, you know, they may have been to a dentist that, you know, there might be like ten different data silos that they've, you know, been to and those silos don't talk to each other. So, really, the patient is, I think, a critical linchpin here. In terms of the matching tools, I think those are all interesting in the pattern recognition, I think those are all good tools. They're already in use today. I think it's the link analysis. There's a company, ID Analytics, that does a lot of link analysis right now in other sectors and that kind of thing is what I think would be helpful here, but it almost doesn't work without the participation of the patient. That's the chink in the armor. That's the hard part here.

>>Morris Landau
All right.

>> Betsy Broder
It depends, Can I ask you what you mean--? Can I go ahead? So, for example--well, I'll give you a good example. There was a really well-known case where one particular criminal went to 83 different providers and used identities.
This was a real problem for the victim to say the least. How could 83 different providers find out about this incident without talking to each other? Is there a way that some kind of reference could have been used to find this person? Well, in some cases, I think there could have been. Not this particular case, maybe not. But for example, let's say you have abusive pharmacological agents and perhaps there's a pattern there that could be derived from pharmacy use or prescription filling. Maybe, there's a pattern there. Maybe, there's a financial picture that could be added. So, that's what I'm saying, link analysis. But this is a very big challenge here. That's why it hasn't been done yet. And of course, here's the big caveat. This is health care data. It's a little bit different than a credit card number so that's the challenge.

>>Morris Landau
Agreed. I want to follow up on what everyone has said particularly when you're talking about--Pam, you'd mentioned the fractured system. You'd mentioned about the person went 83 times and Betsy, you mentioned that it's an open system so I want to go a little higher up 60,000 feet and talk about technology and the possibility of governance in the NHIN and the possibility that systems can talk to each other so people are aware of things. So, as for building the network of networks in the National Health Information Network, can you address sort of the notion of the theme of accountability so we can break down some silos? Anybody wants to jump in?

>>Liesa Jenkins
Being one of the HIEs that is participating in the NHIN--it's enough acronyms for awhile--we're actually involved in the consumer empowerment, use case and are trying to work through in and understand what, how, when the patient can access this information in a way that interacts with the clinical system so that there is that check step because I agree with Pam that the one person who truly does know what reality is that individual regardless of what the records say.
The governance within the NHIN--as I said, you've got governance issues enough, problems enough administering in an individual organization. You take that to HIE level of whether it's national or regional or whatever and then that is multiplied and then connect those together in NHIN and it's almost mind-boggling. But I have a plea from those of us who are trying to do this that, you know, we have identified some of the issues. I think there are some recommendations and there is some consensus coming forward out of that project. Please, please, let's look at this at a national level rather than a state by state level. The worst thing possible that we could do is have 50 different sets of

laws regulating what happens when there is identity theft or there is a breach or, you know, what's required, what's the baseline you have to have. Maybe I'm more sensitive to that because we live in a region that's a multi-state region where we already have to check multiple states.
I think it's an absolute necessity to have a national solution about this.

>>Morris Landau
Other folks?

>>Pam Dixon
Okay. So, it's a thoughtful question and I appreciate it.
At the June forum, I think you watched me schlep around and ask all these questions and annoying everyone--

>>Morris Landau
What goes around comes around.

>>Pam Dixon
I know. There are a couple of thoughts.
I think, you know, one thing I could definitely see from doing that is that this is not been baked into the NHIN. I'm sorry to say, I mean, in terms of the technical specifications and the technical standards at the very lowest level like the zeros and the ones level, this is not there. The only thing a victim can do is get the record deleted. So, I think that now that you've done this and brought more attention to it--and by the way, thank you very much. I think this is a very important effort and I really appreciate it and thank you for it.
I think there are three things we can really look at. One is correction. Second is access. And the third is transparency. I think that because we've got this problem, we've really got to take a cue from the Fair Credit Reporting Act, not to say that we need to apply a blanket over this which would never would work, but, you know, I do think that patients do need to know where their information is going at a fairly granular level. I know there's a lot of push back on that but we've got to get a handle on that. So, I think that those are three things right there that we could focus on and figure out at the NHIN level. That would be very helpful.

>>Denise Tauriello
Others? Lisa?

>>Lisa Gallagher
I think one of the things we do is think about the NHIN as a service provider in a sense that there are perhaps some network services that can be part of the business model of the NHIN.And this is an area where we can consolidate what we're doing with regard to identities and things like that and, also, perhaps even, as Pam mentioned, you know, a way for one consolidated process for patients to provide their inputs when, you know, my record isn't right or I've seen a strange pattern, etcetera. And even if we don't solve the whole thing, there's sort of a

collective, you know, look at the problem and maybe even a role for the NHIN as an entity to play, to provide service to all those entities that are connected to it including the patient.

>>Harry Rhodes

Even though the NHINs are at a state level or a national level and maybe even someday at multi-national level, I do think that there--it isn't totally out of control. There is a community. There are common stakeholders. People do know each other and I think through the data use agreements and the data sharing agreements and all the other participation agreements, you can't set expectations and set in security controls and even mechanisms to respond and act on things. And yes, absolutely, I do believe that standardization is really important. I know that everybody wants it their way but this is one situation where agreeing upon one way to go would really benefit the ability to monitor it and act when you do suspect some thing's not going right.

>>Lisa Gallagher

And I guess--I just have a very high level of response to what Pam said because going back to the very beginning and Jodi's comments, we wanted to look at prevention, detection and remediation of the harms that are associated with medical identity theft and then look--and so to find--I don't think any of us believe there is a silver bullet that there's one way but maybe guiding principles as Pam described them of access correction and transparency or at least help inform the choices that you make as to how they fit in that these are as Pam says baked in to whatever approach one has and how everyone builds a system rather than duck-taped in, you know--well, I guess you don't duck-tape whatever you're baking but applied after the fact--icing, thank you--that I think would take us a long way.

>>Pam Dixon

I would say we need to talk to the actual consumer though. I think part of the reasons of financial identity theft issues have worked out so well, I think the Federal Trade Commission has done a really, really good job of asking for comments and really getting a very broad swat of public opinion.

I think that would really need to take place. We've got to talk to the actual victims here and the people who are really involved in the process. They do have an opinion. There are real harms right now. Not tomorrow, but right now. And I think that the people who've been victims of this crime actually have a lot of wisdom about how this could be fixed.

>>Denise Tauriello

Good point, thanks, Pam.

Before we leave the data issue, I heard today around the Data Integrity Committee that I believe Massachusetts has in place.

Harry Rhodes, I know, he’s sitting next to me, also talked about data integrity and that becoming a unique role within organizations.
I’d like to explore that a little bit as a possible next step or that role both as in the form of a committee and as actual individuals within organizations.
If Shanda, you can lead us off and talk just a little bit more detail about what is the role of that committee in your organization, how did you end up setting it up, if you can sort of make that concise, that will be great.

>>Shanda Brown
Sure. The role of the Data Integrity Committee at Mass. General is to look at all issues related to patients, integrity patients’ data. That includes fragmented records as well as overlays as well as wrong medical records, anything and everything that might affect the patient, clinical decisions that are made that might have a downstream effect on the patient’s identity, so things like when a patient comes into the ED as a trauma patient, how and when we decide to put a name to that patient so as not to compromise patient integrity when we’re trying to treat the patients. So, all of those issues fall under the broad umbrella of our Data Integrity Committee. It’s a multidisciplinary committee that we created. It has members of the HIS department, members from police and security, members from information systems, the clinical departments as well, radiology, EKG, lab, registration. So, we bring all those players to the table and we meet on a regular basis to discuss any issues that come up through our departments as well as being a resource for the hospital if any other department--say nursing has an issue that they would like some insight on.

>>Betsy Broder
Have you found that to be beneficial? I mean have you seen a change? And I know you guys have been starting to track medical theft cases in particular but maybe you haven’t enough runtime.

>>Shanda Brown
We found it to be beneficial for several reasons. One of which is it does provide one committee as it were to address these issues where we’re all already in the stand place. And one of the reasons this came about is we were sort of fragmented in dealing with several different issues that’s sort of distilled down to the same root cause of data integrity and found we were meeting, you know, several different times a week and the same people at the table all those different times and said, “Wait, why don’t we just create one place so we can all discuss a variety of issues,” because we found a lot of the issues we’re dealing with and some of these I just mentioned all the same root cause and the integrity of the patient’s data.

>>Shanda Brown
At this point in time, it’s a little too early to tell. It’s a relatively new committee. So, we are looking at that. We're starting to track some of that. We’re putting together

right now sort of our dashboard of what we would like to see in terms of those numbers. So, give us a year or so and we'll have these numbers for you.

>>Betsy Broder
Are there any other metrics that you're going to use to track your effort?

>>Shanda Brown
Sorry?

>>Betsy Broder
Are there any other metrics that you're going to use to track the success of your committee besides, you know, clinical outcomes, anything else?

>>Shanda Brown
Well, we're also looking at just--some of the things we're looking at is there's some issues right now related to payments and things like that that we're also tracking. Like I said, the point of the committee, and it is a new thing for us at Mass. General, was to create a single location where anything both on the clinical side as well as on the demographic side could be addressed that had a data integrity impact.

>>Denise Tauriello
Great. Thanks. Harry?

>>Harry Rhodes
Earlier, the panel, we talked about ideas that we can take from other professions or other industries and the idea in management is that if you want to get a job done, you have to give the employee ownership for the task.
I think that's one of the reasons why this idea of having a data integrity specialist or employee or a data integrity specialist team really works because you're actually giving somebody ownership for it. And I also think it's also the reason that supports Pam's argument, the reason that the consumer is a good stakeholder bringing into this is because they have ownership in this process. And so, that's really a driver in it. It'll help guarantee success.

>>Denise Tauriello
Great. Thanks, Harry. Anyone else? Betsy, any other questions?

>>Betsy Broder
No.

>>Denise Tauriello
Okay.

>>Betsy Broder
Not at this moment.

>>Denise Tauriello
Thank you.

>>Lisa Gallagher
I have one comment about the data integrity. Having attended again, I'm--and I'm a big fan of some of the professional associations of folks. This is what they're trained to do. I mean they're the experts in the field. They know what it's like today. They know where the problems are and they probably sat there and thinking at lunch, thought about some of the solutions. And there is an association for health data integrity. It used to be the Transcription Society. You know, they're looking at, you know, how is our profession evolving and where do we go. And I think to tap the people who are going to be evolving from one role to another role within this profession, within this industry, is probably a smart thing to do.

>>Betsy Broder
Great. Thank you. Back to you, Morris.

>>Morris Landau
I've got--like we're on newscast here.
Let me just say that--sort of a very high-level question but it's purposely so.
And what we haven't really touched about and I would like some specifics on education and training and I want it from consumer perspective, provider prospective, IT prospective, what the government perspective is, because what I'm hearing throughout this session is that it's a collaborative process to deal with this issue with consumer being the center of that. So, if you could address what can be done specifically about education and training and then part two, simply because I have a short airtime is, is there something we can do about EOBs and that sort of ties with that as well and how can we make it consumer friendly?
So, how about it, whoever wants to sort of deal with education and training piece.

>>Morris Landau
I can't believe this.

>>Denise Tauriello
You stumped them.

>>Morris Landau
I stumped the panel.

>>Pam Dixon
You know, where I would start, maybe--I think the consumers learn when they feel it's necessary for them to learn. It's kind of, you know, is this relevant to me

now or not? And so, it's at the point of contact where they're interacting with the health care institution, that's a good opportunity for educating them and training them and that does place a burden a lot of times on the Health Care Provider Organization to be that educator of the consumer but that's where it's happening today. The big place that I see a gap in understanding some of the issues around particularly health information is among the policy makers. The very people who are trying to draft laws and get them passed because some constituent comes and, you know, you've got this hodgepodge of very well-meaning folks in of positions of authority who really don't understand the issue or the potential solutions. And so, I hope that there is some mechanism for really helping bring our government officials to a better level of understanding about what needs to change.

>>Betsy Broder

This is why I didn't respond right away in terms of consumer education.
It's because the message is so hard. The message is so hard because there is not a structure now for consumers to control their environment and the way that they might in the financial sector. And so, we're talking about this. I was talking with some colleagues about breach notice in the context of health care. And dear Linda Foley, we're very sorry to tell that you that your information has been breached. You may want to put fraud alert on your credit report, blah, blah, blah. Also, your health information has been breached. Good luck. You know, so, because the remedies aren't there, it's much more difficult to convey the consumers' information beyond. Be very careful with how you use your data. If you have, in this context, medical identity theft, if you have critical health issues make sure that every health provider you encounter is aware of them in the event. Having said that, we don't want people to be in constant state of hysteria that this is happening to them. They need to be balanced. They need to understand when it's important to address these issues but they should not feel that they're always, you know, this close away from becoming a victim of medical identity theft. So, you know, finding the right time, and maybe as Lisa said, it is finding that right teachable moment but probably some baseline information that would be helpful for everyone to know. But again, it's so difficult to say because what is actually the message, you know, that we're conveying to them.

>>Pam Dixon

We really faced this in California when our breach notification laws were expanded to include medical data and basically I was asked by a multiple people on the state. Well, what do we tell them to do other than worry? You know, and that's unfortunately a legitimate question. Regarding your question, I think the first thing I would say about education and training is that consumers need a place to go preferably in the Federal Government. We send everyone to Federal Trade Commission to file complaints in the consumers' sentinel. I think that a lot of CMS, they go to the OIG. So, we have a couple of different pies that are collecting, you know, consumer data. And that might be worth thinking about.

Where do we want consumer complaints to go? Who's handling consumer complaints? And where's the logical place? We've seen a lot of overlap in types of identity theft. So, people who have medical identity theft often have financial identity theft. So, I think certainly some cross-pollination would be very helpful, for example, on the OIG website to link to the FTC's website information on identity theft I think would be very helpful because there might be a real correlation there. Betsy's comment about there's not a structure for the consumer to change their environment; I think it's really critical. I think one of the things that--one of the few proactive things we can tell consumers to do is to get a copy of their health records before they need to. That is the one thing we can do but that's a really hard message to get out. So, we almost need to agree on a message, you know, and then where to place that message, at a federal and state level, and then, you know, how to agree upon some solutions for and remedies for consumers. So, we actually really do need to take that remedy step at some point sooner rather than later.

>>Betsy Broder
And I'd like just to add the whole idea of complaining to the FTC. We're probably the only folks who really like to get complaints. And we have established toll-free hotline for victims of identity theft and an online complaint form for victims of all sorts of identity theft and this serves a dual purpose. First, when the consumer contacts us either online or through this toll-free number which is 877-ID THEFT, they are connected either with the person or with the website that provides substantial information on how to respond to and address the problem of identity theft. This quarter of a million complaints that we collect every year, we make available to law enforcement through a secure network called the Consumer Sentinel Network. So, Criminal Law Enforcement, there are like 1700 agencies that have access to this real-time data and they can go in there and look for clusters, look for connections and it helps them develop leads for criminal enforcement. So, it provides an educational opportunity for the victim of identity theft and it provides data for criminal law enforcement. So, any of you who might be situated in a way where you hear from victims of identity theft, we would encourage you to direct consumers to the FTC and all these resources for consumers both educational, the online complaint form and the call center are available in English and in Spanish. One of the things--a colleague of mine told me that she was hosting HIPAA Brown Bag lunches and it got to a point where the attendance was really dropping off in the HIPAA Brown Bag lunches because nobody was interested. It wasn't a hot topic. We started talking about medical identity theft and how you can use the HIPAA regulations and guidelines to fight the identity theft--suddenly, her attendance went up and not only that, she would run into people in the hallway, "Hey, you know what I did the other day because--fighting medical identity theft." And so, I think one of the things that we can build off of is fact that there hasn't been one person I've talked to yet where I've said medical identity theft to that their ears didn't prick up. This is a hot topic. We all need to decide what gems we are going to share with them. What can we give them of value? I think we should take advantage of the fact that this is a hot

topic. This is a burning issue. People are interested in it; unlike a lot of other advice that will probably, you know, fall on deaf ears.

>>Morris Landau
I just want to do a quick follow-up really quick and that is you talked about consumers. Let's talk a little bit about providers and other stakeholders because you mentioned data stewardship and it starts with consumer but there are other stakeholders involved. So, can you address about consumer, I mean education and training for your local physician, your local health care provider, local hospitals. You could talk a little bit about how other folks who have access to health information can be trained, addressed, etcetera.

>>Pam Dixon
I have a pretty basic thing. I wish Calvin were still up here. But the ones who stand to lose a lot if the providers are not doing what they need to do are those that insure those providers and those patients. So, it seems very logical that insurers of providers and patients would be champions for educating providers about what to do to protect a patient's identity. I don't know if they're doing that very comprehensively or not; but if not, I challenge them to step up and start. And I think also it's just important that we have a responsibility to maintain trust with the patients that we see. So, you know, educating patients on this issue from--as a clinical issue--is important just in the sense of continuing to build that trust with patients, letting them know that we are on their side, you know, we will advocate for them in the cases where this happens and helping them work through the process and educating, you know, consumers if they become a victim and where to go the next step. So, you know, I think that's very important from a provider level that we do have that, you know, procedure in place to be able to provide that level of, "Yes, we're here to help. Yes, we're a resource. Yes, we know something about this if it happens to you," so they have some place to go.

>>Denise Tauriello
Thank you very much.
I have sort or an interesting question. It's slightly different than the ones we've had so far. Maybe, it won't stump the panel. What are possible funding sources for researchers wanting to work on potential solutions? Who's going to go first?

>>Pam Dixon
You know, I think I'm going to rift off that question a little bit.
I think the one thing I'm kind of dreading seeing is medical identity theft becoming some evil profit center where there's all these cottage businesses and all.
We don't need that. Academic research's great. But, you know, I guess I've been kind of influenced by a vendor who came by and just insisted that all consumers needed to sign was this, you know, really powerful power of attorney so that they could go fix their records for them. I don't know. I would be very supportive of academic research or research that was done in the public interest. But in terms

of other things, I'm going to leave that to the providers to answer. This should not be a profit center.

>>Harry Rhodes
I think there already exists a great deal of time and money that goes into fighting medical identity theft that's just not called that. It's called, you know, systems security and privacy and confidentiality. And I do think that--I think those groups are mindful of this problem and I think they are trying to have the solutions but they don't necessarily call it medical identity theft. They call it by a lot of other different titles instead.

>>Lisa Gallagher
I agree with Harry and I would go even further. I'm not sure we need "research." I think the emphasis really needs to be on the education and training. To me, as a security practitioner, this is a risk-analysis issue. It is, you know, recognizing this threat, understanding this threat source, the threat motivator and factoring that into your risk analysis. And so, if people don't understand the way that I just phrased it or what I just said that's what they need to be educated on is that they need to--this is a business risk and this is a security risk and they need to approach it as such. And if they incorporate it into what they do and, you know, as an organization dealing with their own business risks that will hold them in good stead. Not that you don't need special expertise and that there wouldn't be technology that would be applied. But they have to recognize it for what it is and they have to have data that they get on the threats. They have to look at their own vulnerabilities and mitigate those appropriately. So, the education around incorporating, you know, security and risk management practices and keeping their employees educated and trained on it so that they're part of the process I think is the most important thing. Other than that, I don't think there's anything new here other than the clear recognition of this particular threat.

>>Denise Tauriello
I think that's very valid, Lisa, but how might we do that? I mean, how might we--what would be a mechanism for bringing forward the unique issues around medical identity theft and in particular, into the risk assessment process in a broad, you know, in a broader scale?

>>Lisa Gallagher
Well, I talked a little earlier about how I think this industry has been a little slow to do some collective, you know, data-sharing on threats and vulnerabilities.
And I think it's--I'm not really sure as to the reasons why and maybe it's, you know, along the lines of what Betsy talked about when there were the right kinds of motivations and incentives for the organizations to do so. And when they start to get some information on the amount of money that they're losing and the threats to their patients, you know safety and, you know, maybe that might, apart from all the other times that we've tried to share threat data in this industry and we just haven't had any interest. This is really something that it's a new and

emerging threat. It has a potential to be huge and do tremendous harm to other patients. And at some point, you know, we need to come together, you know, the large providers, the payers, the academic institutions and really take a look at, you know, what this threat is, what forms it takes, how are people motivated, when those things shift so that we're following patterns of threats. As you said, you know, it changes from one day to the other and sharing that information so that we can fight it together. You know, to me, I think that's--so, an industry solution. I mean we can put all the laws and regulations we want in place but if we're not actively fighting against this by recognizing it and factoring it in and sharing information, I think they're always going to stay one step ahead of us. So, and in coming together, that is an educational process. Information sharing is an educational process. So, it's a combination of talking about the, you know, risk analysis techniques but also actually sharing true data on what the threat looks like and, you know, what our vulnerabilities are in our current system and, you know, working on it.

>>Denise Tauriello
Great. Thanks, Lisa. Anyone else?

>>Denise Tauriello
Thank you. Back to you, Morris.

>>Morris Landau
Yeah, I want to talk a little bit about remediation and what we've heard from our research is we would talk to victims. The victims would find out ninety days, six months after the fact that their identity has been stolen.

>>Pam Dixon
Though we usually receive something from a collection agency, something to that effect. And one of the challenges that a victim has is trying to convince law enforcement, particularly local law enforcement. But my question is, really, how can we help the victims and what can be done about trying to remediate what has happened to them? And part of that question is also the--which we just touched upon, "What happens when medical identity theft occurs to a victim?" because I think that story needs to amplified as well. So, the bottom line is, what can be done about, not just law enforcement but, really, at a local level as well? Anyone?

>>Pam Dixon
You know, we've dealt with so many victims at this point; what I can tell you is that this, you know, this kind of fraud has been around a long time, but I think what hasn't been around a long time is an acknowledgement of the impact this has on individual lives. And I just--it's not possible for me to articulate fully what it's like for this people because it's not happened to me to the degree that some

other people have had. I think something that we need to do for a victim is that we need to have--and I'm going to go back to this--we need to have a process in place where we listen to what they have to say and it's really the first line of defense for victims are the providers. I can almost predict what kind of phone call we get. And this is kind of how it goes, and I think I've already said this today. First call, "Oh, you won't believe what happened to me." "Tell us. Okay. Tell us." Next question, "We can't get our medical records." And then, you know, walk them throughout the steps. And then they'll come back and they may say that again and they may have to hire an attorney to get their records; it's not uncommon. Then after that scenario is finally played out, either they give up and just never get it corrected or then they come back and the very next thing they have in place and--is--"Well; now we can't get any kind of amendment. We can't get changes. The hospital doesn't believe us. They think that I'm the one that did it." So, basically, there are a lot of problems with no one believing the victim, including the hospitals. So this is not uncommon. And I think what we really have to do is work with victims, people who have actually been victims, consumer stakeholder groups who work with victims and say, "Okay, here's the victim experience. Here's what you could do to help. I can tell you one thing right now that would help so much, is figure out a national level procedure for getting records to victims." People who come to your window and say, "I'm a victim of medical identity theft." Okay. What is the response?

Is there a five-step response that a victim can expect at every hospital? Because, right now, they're getting different responses and, usually, they have to go to multiple providers to get this thing fixed. So if it's a national level, you know regular response. But the next thing is the collection agencies; this is a collection disaster. And I think Linda probably has hair-raising tales on this.
Anyone who has worked any victim at all on this will have tales to tell about the collection agencies. You'll go to the hospital and say, "I owe you $150,000, what?" And they'll say, "Go talk to our collection agency. It's out of our hands." You go talk to the collection agency and they'll say it's you; it was your Social Security number. You go back to the hospital and there you are, you are ping ponging back-and-forth and it's just an absolute nightmare for this people.
And we actually have had victims who paid the bill; the smaller bills under a thousand dollars, just to get this off their credit report and to get the collections out of their life and from ruining their life. So I think simple things like, "How does a hospital handle collections? How does a hospital handle the liaising with law enforcement?" That's a huge deal. When victims that we worked with get a police report and get local law enforcement to believe them, they'll take you to the hospital and the hospital has no mechanism to accept the police report. Something that hasn't been said today that I do need to say, that's very intriguing to us and we have a number of hypotheses as to why it is so, but we have not gotten a single complaint. Not one--not in three years--from a victim from a small doctor's office. Not one. They have all been from larger institutional providers. And I think that that's a very important point to keep in mind and our top theory as to why this is--and by the way, we have no data to back this up. None.

It’s just a hypothesis. The hypothesis is that people go to their doctors and go, “Oh, look what happened?” The doctors know them. Or they just look at it say, “Oh, let’s fix this,” and it gets resolved right then, right there. So I think that’s something very interesting to look at. Why is it working there and not working in other places? Because we’ve talked to smaller providers who have seen this but we’re not getting the complaints. So I think that’s an intriguing issue.

>>Liesa Jenkins

One quickie… you mentioned a relationship between the providers and the law enforcement agencies; I do think that’s a place where the professional associations or the health information exchange can play a role.
The folks who are experts in the fields of security and compliance advised our health information exchange to reach out to the local FBI and to educate them in advance far before we ever became operational to exchange information to educate the local law enforcement agencies about what are we talking about doing, who are we, why are we doing this, so that if someone--if something does happen, it has--yeah, but if something does happen, they’ll at least know who we are and, you know, the background, then we won’t have to start from square one to convince them, you know, of--that this an issue that we’re trying to address.

>>Denise Tauriello

And then I’ll get to you, Linda.

>>Linda Foley

I think that part of the problem is we need an overhaul the way we do our investigation instead of automatically assuming guilty until proven innocent.
We should have a better investigation process. And, in our response team, I was going to add that, yes, you should involve local law enforcement, you should already start making those connections. I thought it was really interesting that I was out of the FTC site and they have forms that you need to fill out if you’re a victim. But they also have a cover letter, open letter to law enforcement which I thought was a really good educational tool and I think it would carry a whole lot of, you know, it carries a lot more weight than you just standing there by yourself trying to explain what happened to you. I think that--it also, the open letter also includes actions for what you should be doing. So I do think that organizing a response team, bringing together all the stakeholders which include law enforcement, and doing that thorough investigation before you automatically jump to conclusions is probably the best advice. And one thing that may complicate this a little bit to the extent that a certain amount of medical identity fraud takes place by someone known to and close to the victim. And that’s the police report, which can be essential to someone who is recovering from identity theft. And people maybe vague on some instances. They maybe very willing to get a police report--again, someone who has done this--but there are maybe circumstances under which they’re less apt to get a police report if it could involve a member of their family. And so, that’s one consideration.

But the other one is, we've been spending a lot of time at the FTC working with the FBI, Secret Service, Department of Justice, others, training the local law enforcement. In fact, Kate Claffy is here we've--she's done more than 30 outreach programs for local law enforcement around the country. And part of it is the same cultural change that is explaining to them that, "Yes, there are remedies for fixing problems associated with identity theft but these people still are victims of crime. Even if they're not out of pocket, there are serious consequences that flow from all types of identity theft." And it is essential that they write police reports; that are a mantra that we repeat over and over and over again. But still, I guess, you know--Linda could comment on it and maybe Pam--people have a hard time getting these police reports if it appears to the police that it's either a family or a close person or that the consumer has other remedies so it's really no harm no foul.

>>Morris Landau
I know Linda Foley wants to make a quick comment. You need to probably speak into the mic because…

>>Linda Foley
Police reports, we don't have a hard time with this, much thankfully… partly, because of the FTC. And I work very hard with family cases, so I get them changed. The minute we get a collection notice, we use that to start the police report as financial identity theft. Taking it from there, we can go to the collection agencies and use the Fair Debt Collection Practices Act and get them to back off of that way by showing, "I couldn't be that person. I'm in San Diego; I was not in San Jose. I was working that day, showing the alibi." "You had your appendix removed?" "No, I will be happy to go through an ultrasound and show you I still have my appendix." It's showing the facts of the situation and then the health providers back off very, very quickly. We don't have a hard situation, but we have had people who do commit suicide over identity theft.

>>Denise Tauriello
Yeah, we've gone…so I have a good wrap-up question.
This has been a great dialog and I think, you know, as Harry mentioned earlier, this is, you know, the beginning of a process of starting to share information collectively as a group of stakeholders. So my question then is, "Where do we go from here and what should the approach be to continue the dialog and to continue the sharing of information?" Is it a number of different things?
Do town hall settings like this, or are they helpful? Is this one place to start?
What else can we be doing specifically to ensure the dialog continues? Anyone?

>>Harry Rhodes

Well, it's--HIMSS and us--at AHIMA, we work together quite a bit on different initiatives and we've—at AHIMA we have become accustomed to working with other groups to come up with solutions, especially tool kits and guides and I would love to see us do something on that topic--on this topic, you know, bringing together the stakeholders and come up with some hard and fast solutions because that's obviously what everybody is looking for. And once we, you know, collect the tools and mechanisms that we can share, HIMSS and AHIMA are… You know good distribution mechanisms to the provider organizations that need these materials. So, you know, we have tool kits and white papers and case studies and all that on our website and we'd be happy to, you know, help facilitate getting the information that we developed out. And I sense from even being here today that there's probably some information available that we could, you know, collect from Pam's group and from FTC and, you know, put it all in one place. We can also do educational sessions you know, things like that just to get the providers on the line and say, you know, "This is a threat. Here's what we know. Here's what organizations have seen so far. Here are the, you know, national level efforts where we're going to bring stakeholders together. You know, maybe a next on the series town hall, those kinds of things.

I think communication on the issue right now is, you know, the awareness issue. It's really the stage that we're at. I sense that with the provider organizations that we surveyed. We really are in an awareness phase. And as much as we can bring some solutions to them, we have to get them to look for this and know what to do when they find it.

>>Betsy Broder

I think positive incentives go a long way. So, I think there's someone here from the American Hospital Association, right? So, yes. Okay. So, what Massachusetts General Hospital is doing should be showcased. And when you have data that shows what a fabulous success this is in terms of patient outcome and fraud loss, and all of that. That I think would motivate at least, you know, larger systems to take notice and to see that it really does--first of all, it could be a marketing advantage to the extent that there is competition out there. But also, it's the right thing to do. And it could have other incentives. And so, I think there is an opportunity there to use entities that already have identified the system and establish your processes in place to identify, detecting and remediate these forms of fraud.

>>Denise Tauriello

Thanks very much.
Morris?

>>Morris Landau
Just sort of quick wrap up. I'm sorry we couldn't get to all the questions.
But I want to thank everyone on the panel for some very meaningful dialogue and discussion. And we really hope that this is a starting point. So, again, thank you for everyone's participation. And I'm going to hand it back to Jodi for some closing remarks. Thank you.

>>Jodi Daniel
Thank you so much everyone for participating. This has been really quite an exciting day and exciting discussions. When Morris and I were first talking about medical identity theft and some of what we might be able to do. And talking with Betsy further and some of the folks of FTC about what we know about the issue and what might be a good opportunity. We did realize that we really are in an awareness phase and that what we need to do is make sure we understood what the issues were and raise awareness of this issue before we figure out what's some of the next steps might be. And I think we really accomplish that.
Harry made a statement which I noted down because I found it really interesting. He said that even though he's been standing this issue for some time now, that he's learn so many things here. And so, that was really encouraging to me. That even, you know, some of the experts here are learning new things by having this dialogue. We really--when we decided to bring up this issue, we had some folks at HHS who pushed back and said, "We thought that are stepping in a big can of worms. And we really pushed it and said, "You know, this is an important issue and we want to take it on proactively. We don't want to wait until there are some crises." I understand that there are a lot of incidents already, but, you know, when there are some big medias flash crises that we have to react to, we really want to take it correct and look at this issue and start this discussion not in a response to a crisis. And then there were other folks at HHS who said, "Can you get it done faster?" We originally had a longer delay in getting this fold together. So, I personally want to thank Morris Landau for his heroic efforts of pulling this off, and also, our Booz team, Booz Allen Hamilton team who have been working diligently to pull this off under much constraint timeframes that we have put on them. I want to just do a little bit of wrap up and kind of identify some of the things that I've heard just to follow on to the last comment, the last question that was answered. I heard suggestions for next step about tool kits and guides using some of the industry folks to take leadership for all the leader educating their membership or coming together to try to think about industry standards that can help in this area, educational sessions with providers. Another town hall, we'll see if that--if we can pull that off. Using positive incentives trying to showcase some positive--some good actors and people who are trying to take this leader--this issue head on and take leadership in this area. The thing about the role for the NHIN, which I will personally take back as--to do, so in work with some folks back in my office on that, Federal Agency leadership. And hopefully, Betsy and her team will continue to work with me and my team to try to think through that. And especially important to make sure that we're engaging the consumers and doing that directly and aggressively and not taking

them for granted as we’re thinking about this issue, but really bringing them into the fold. A couple of the other things that I heard that I just want to wrap up with this, that the statistics on medical identity theft are scarce. And I’ve heard some call for--for a need to better understand the scope of the problem, the actual impact of the problem. I heard some comments about, you know, what is--how many errors really are there in people’s medical records and what kind of impact does that have on care. And that we don’t have good numbers for that. And I’m encouraged because I also had some folks come up to me and say, “Hey, you know, we have some data that might be helpful for you or can we work with you to--to try to see if, you know, that data we have from collection agency might be able to help you quantify the scope of the problem. So, I think we need to think about how we might study this issue better so that we’re acting from knowledge rather than from just anecdotes. Of course, importantly, I heard that this issue can have devastating impacts. It’s--can have significant, significant effects of the individual to the point of, you know, we heard a victim talk about the fact that years later she’s still fighting this issue and trying to clear her records and her financial and medical records. We’ve heard that individuals don’t have good remedies. There are some gaps and the consumer protections in what they can do to address the issue and in--in understanding of those, even who do have obligations to provide access to records, understanding what those obligations are. So, if the consumers aren’t trying to fight with the--the folks are holding the records to get those records corrected. We also heard that one of the other challenges the consumers have is that, the theft can continuous. So, even if they cure the problem, there could be some downstream problems, their information can be sold to others and that it is almost, it could be near impossible to get a hold of the, the horse once has left the barn. We’ve also heard that there’s no single answer to this issue. It seems to be--I’m both energized by the conversation and all the ideas that came up.   And also, I think a little bit nervous about all of the issues that came up and have or get to try to prioritize and take them on. One thing that I think is critical is that, I think we start to develop a community to discuss these issues. And I think we need to continue this and that’s something that I would like to think more about how we can best do.
I heard about clearing house for best practice is raised as an option and, you know, thinking about creatively how we might be able to use technology to continue the dialog in addition to these open forums. We’ve talked about some concerns of the technology can have some positive impacts, we can use technology to help prevent and detect identity theft, but that the technology also brings new risks and we need to think about how we do, how we educate providers about risk assessments and continuing to do those risk assessments as the risk change over time. I’ve heard--I heard conversations about needs for uniform processes and concerns about different processes by different providers, different laws in different states. And that one thing would be very helpful is some more uniformity in this area. What else do we hear? A whole lot of things. Education and awareness. Education, education, education. I think the one thing that we were hoping to achieve with this is you start doing some education and raise some awareness about this. I know that there were some press

interests in this town hall. And hopefully, there would be some media attention to this. And there will be more press about this and you will have more people who are saying; “I heard about this thing of medical identity theft.” Is this something I should worry about and how do I deal with that and, you know calling up Lisa and getting some best practices in that sport of thing. And then, we ended with how health IT technology can help. We talk to a little bit about using pattern recognition and how that can help the detection, prevention and detection, like it’s done in the financial industry. But I also heard about the need to have that is dynamic, so that as the lessons learned on how to you know use the system that the recognition and the detection activities and processes can keep more with that. I heard a call for guiding principles, particularly in the area of health IT as we’re building with health information that work, make sure that they’re guiding principles that are underlying them particularly in the areas of correction and assess, and transparency. Again, something we even been talking a lot about privacy and security in the any and that is something that I hope that we can take, take it to heart and take--and do something about. We’ve talk about patient identification and authentication, and again the risks that can happen there as well when people are collecting information to identify an authenticate providers and patients, and if that, when that information gets combined with the patient record and having to figure out how we make sure that any information that’s to identify an individual is not then vulnerable as well. So, a lot of stuff. And, like I said it’s supposed the exciting and overwhelming. Our next step is that, we have the team--you know and see working with our Booz Allen team is going to try to digest some of this, come up with a report that both brings together all this information and brings forth some of the recommendations that are come out of here, and some of the suggested next steps that we can then use and make available publicly. We do have, as I mentioned it in the beginning of the meeting, an environmental scan that has been put together by the—Booz Allen team on our behalf. Those are available outside, it will also be up in our websites, so please don’t forget to grab a copy when you walk out today. I think, you know, when we read that over again tomorrow, we’re going to realize that what we knew yesterday was a lot less than what we know today. So, hopefully our final report would be much more informative and be able to incorporate some of the more complex things that we talked about. And, I want to say that a lot of people have come up to me personally and come up to other folks in our team, and ask how they can stay engage. And I’ve got a bunch of cards, I’m sure other people have a bunch of cards. What we will try to do is, we’re going to have to go back and regroup. Whatever next steps we will plan will make sure our publicly announced on our website if there are opportunities to stay engaged, we’ll make sure to make those available. We do have a list serve at www.hhs.gov/healthIT. And on that list serve, we do make announcements about any public meetings, about any opportunities can involve and things like that. So, I encourage you to sign on to that if you’re interested in staying engage, and if there are opportunities, we will definitely make them available to that list service while as to our website. So I just like to close and thank everybody for their participation. Particularly our panelist and the team of folks who pulled us off. And I look forward to working with many of you in the future as we start taking the next step on this past forward on dealing with medical identity that's been coming up with some solutions. So thank you very much.