WORLD **PRIVACY** FORUM

Keynote Speech

Medical Identity Theft: Issues and Responses

AHIMA National Convention
General Session
October 9, 2007
Philadelphia

Pam Dixon,
Executive Director, World Privacy Forum

Good morning. Thank you for the invitation to be here today and to speak with you about medical identity theft. Medical identity theft is a crime that harms people and it is a crime that hides itself. This combination makes medical identity theft an insidious crime. It can cause extraordinary damages and harms to its individual and institutional victims. And once begun, the harmful effects of this crime can linger in the lives of its victims for years or even decades. And that is why I am particularly pleased to be here, because I view you -- the leading health information management professionals -- as the key individuals on the front lines of this crime. AHIMA may be the single most important group for finding and implementing appropriate responses to the unique harms of medical identity theft. So it is with great hope that I speak with you today.

Today, I will talk about three things: first, what medical identity theft is and the harms it causes. Second, how this crime is operating based on the latest research. And third, I will talk about best responses and the key role you can play in that process.

So, let's begin with the question: what is medical identity theft? Medical identity theft occurs when someone uses an individual's name and sometimes other parts of their identity – such as insurance information, SSN, and so on -- without the individual's knowledge or consent to obtain medical services or goods. Medical identity theft also occurs when someone uses an individual's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

In its simplest form, medical identity theft can be committed by an individual acting primarily alone. A common scenario occurs when an individual walks into a clinic or other health care provider and uses someone else's identity information to get treatment. The information the identity thief may use can consist of a name, home address, an insurance card number or social security number or even someone else's health care file. An example of this is what happened in the Missouri case of Julianne Sample. In this

case, Ms. Sample stole an identity, went to a regional hospital, altered the victim's medical files, and got prescription drugs in the victim's name.

Medical identity theft is also committed by groups, not just individuals. There are a number of operational methods that groups use to commit this crime. Typically, groups operate through insider methods. In one example, in the Dzhuga case in California, an organized, sophisticated group of criminals took over a medical clinic, acquired patient information through free exams, photocopied the information, and then billed the victims' insurance over the course of almost a year for conditions the patients did not have and services they did not receive.

The absolute hallmark of true medical identity theft of any type, whether committed by a group or an individual, is that changes based on the fraudulent activity are introduced to a victim's health care records. These can be introduced to the legal health record, insurance records, electronic health records, and the whole constellation of associated tests, codes, and basically any other information that can be exchanged about patients. These changes are as a result of the criminal activity.

Sometimes, the thieves add the information to the files in order to substantiate false billing. In other cases, the changes and inaccuracies to the victims' files occur in the normal course of health care professionals treating a patient, who also happens to be the perpetrator of the crime. One identity thief had a baby and listed the victim -- whose wallet she had acquired -- as the father. To add insult to injury, an associate of the perpetrator apparently used the same stolen identity later for some surgeries. The victim then had a substantial health care file in his name, social security number, and home address without ever having set foot in that hospital.

These changes to the victims' file are the root cause of the harms the individual victims experience. Long after the fraud has been investigated by the provider and long after the last provider's bill is charged off, many victims will still experience the impact of this crime. Victims can receive improper medical treatment based on the fraudulent information in their file. They can fail pre-employment medical exams. Victims may have to file bankruptcy because they cannot get credit after being incorrectly reported as owing thousands of dollars to one or more healthcare institutions. One victim finally paid a fraudulent bill after several years of never being able to convince a bill collector that she was not the individual who had gotten treatment in an emergency room.

I want to emphasize that medical identity theft has two kinds of victims: individuals, and institutions. The individual victims of medical identity theft range from newborns to teens to working parents to the elderly. Anyone can be a victim. Our research indicates that the elderly, the chronically ill, and others who access the health care system frequently or who have had recent contact with a health care institution or provider are especially vulnerable.

Because of the mechanics of how medical identity theft operates, it can often take individuals several years to discover they have been victims of this crime. And once they

do discover it, it is nearly impossible, if not downright impossible, to recover from unless they get lucky and come across a provider or other professional who knows about this crime and how to take care of it. This is where AHIMA can play an effective role, and I will return to that point later.

Medical identity theft doesn't limit itself to individual victims. This crime also has institutional victims. Healthcare providers, insurers, and health care information management professionals are victims, too. The impact of the crime, though different, is no less damaging to institutional victims.

This is a good time to describe what medical identity theft is not. It is not medical identity theft when someone goes into a health care record, steals a name and social security number, and then goes on a shopping spree at a mall. This activity, while it qualifies as identity theft, falls squarely in the category of the financial form of the crime.

I have often been asked about the Eric Drew case in Seattle. In that case, Mr. Drew, while in the hospital, had his SSN stolen by a hospital worker. The information was used to finance a shopping spree. He is definitely a victim of identity theft, but even though the theft of the information occurred in a hospital, this case does not qualify as actual medical identity theft because the information was not used to purchase health care goods or services. The crime did not include the essential feature of medical identity theft, that is, it did not introduce changes to the victim's health care record.

When I first began talking about medical identity theft to heath care professionals, they tended to ask me how this crime was different from the health care fraud that health care institutions already have to deal with on a daily basis. Medical identity theft is a subset of health care fraud. That part is simple to understand. Healthcare institutions usually have prescribed and standardized ways of recovering from health care fraud. Most or all of you here today understand health care fraud and how it operates. Some of you in this room probably have to tackle all sorts of issues resulting from health care fraud.

Typically, health care fraud has been viewed as an institutional problem to be solved. But the reality is that the individual victims of medical identity theft are also left with multiple and challenging consequences of the aftermath of the fraud. The difference is that they usually do not have the skills, tools, or knowledge to recover. We hear from victims who have been arrested when showing up to pick up a prescription, victims who cannot pass medical pre-employment exams, and victims who no longer qualify for insurance due to a diagnosis of diabetes or cancer that has -- unbeknownst to them -- become entrenched in their health care files.

This crime of medical identity theft has unique individual harms for which there is no easy or quick or even established recourse or remedy. This crime falls squarely between gaps in laws. It also falls into gaps in federal agency jurisdiction. Individual victims who have changes made to their health care files may experience both health and financial harms, and sometimes these issues become entangled. So when seen from an individual's perspective, you start to see how there are few, if any protections, for these indivduals

who are victims.

After we published our May 2006 report on medical identity theft, the phones rang off the hook. They are still ringing. We have seen a profoundly striking and consistent pattern of complaints from victims. I'm going to start with individual victims first.

Their first complaint is that they cannot get a copy of their health care files. The second complaint is that they cannot get amendments or corrections made to their health care files. And their files often contain inaccuracies introduced by the criminal. This keeps them from getting jobs, disability payments, and so on.

Unfortunately, HIPAA does not help us here. As those of you in this room will know, HIPAA does not grant individuals an absolute right of access to their health care files. HIPAA does not grant any absolute rights of deletion, even if that information was entered due to activities related to fraud. HIPAA has loopholes and gaps in it that create what can be insurmountable challenges for victims. In our report and in our FAQ for victims, we have outlined in detail why HIPAA does not provide recourse to victims of this crime. What often happens is that the victim will find out somehow that there is a problem and will go to the provider and say: “this file has information not made by me! I don’t have these diseases!” The institution then responds by saying: “we can’t give you a file if it is not about you.”

One victim in Alabama who was billed $10,000 could not get a copy of his health care records after he approached the institutional provider. He had to prove his innocence with a comparison x-ray of his hand to that of the perpetrator’s. This comparison was brokered by a television news reporter, whom the victim had in desperation asked for help. Not every victim will be able to have this kind of assistance or proof.

To show you just how serious the recourse situation is in comparison to standard ID theft recourse, let's walk through a comparison between medical identity theft and financial identity theft. How many of you have ever had to cancel a credit card because you lost it, or it got stolen? How many of you have ever had credit card fraud? Me too. I had a run-in with credit card fraud. A shopkeeper stole my number and went on a shopping spree. What did I do? Probably exactly what you did or would do. After I saw the charges on my bill, I called my credit card company, and I canceled my cards. I got a fraud alert put on my file at the credit bureau. Then, I checked the credit bureau’s files and disputed the errors resulting from the fraud. It took a couple of months, but I got it cleared up.

All of us who have successfully resolved financial forms of identity theft or credit card fraud impacting our lives can thank a key law for that: the Fair Credit Reporting Act and its' recent update called FACTA. These and other laws give us the right to see our credit scores, get a free copy of our credit bureau reports once a year, and give us the right to dispute fraud, inaccuracies, and all sorts of other things.

But -- there is no law that allows victims the same rights of access and deletion of fraud in the health care arena. There is no law that gives victims of medical identity theft the

right to put a fraud alert on their health care files, to correct the bad information in their health care files, or to prevent it from happening again. While victims of financial identity theft can put a security freeze on credit bureau reports, victims of medical identity theft sometimes can't even get access to their health files.

As part of the research for our second report, we are looking for best practice responses to this crime. To do so, we are talking to victims that have recovered from the crime, we are talking to prosecutors who have dealt with this crime, and we are talking to healthcare providers and health information management professionals who are on the front lines. We are accumulating a body of best practices in this area, and we will be publishing this information in our next report. We will also be suggesting some additional best practice responses, and I would like to talk about some of these ideas with you now.

So, let's talk about these responses.

Most institutions that come to us have two things to say:

First, most say they see the problem increasing. Second, they are looking for ways to address the problems that victims have. Everyone I have talked to wants to do the right thing for victims. But here is the caveat: they want to help real victims, but they also want a way to make sure that fraudsters can't game the system by claiming ID theft. We all know that finding the right response here will be challenging. There will always be innocent victims, but there will also be some seeking to game the system by using medical identity theft as a defense. (This may not be nearly as common with medical identity theft as with financial identity theft.)

The first response I propose is a national-level set of procedures to standardize how providers and insurers should handle medical identity theft. The procedures should come from a consensus process headed by the professionals who manage health information. The consensus process must include key stakeholders, including insurance companies, patient representatives, consumer groups, and others. If AHIMA would take the lead here, it could go far to reducing the harms that victims experience.

We need uniform but appropriately flexible answers to these and other questions: what do we do when a patient claims fraud is in their file? What do we do when a patient says the bills are for services the patient did not receive? What do we do for patients and other impacted victims when we uncover a fraudulent operation? When we have a real case of medical identity theft, how can we work with patients to fix the records and limit future damages?

You may be surprised that not all institutions, for example, will accept a police report from a victim, even if the report provides unambiguous evidence that the victim is not responsible for a bill or services that have been charged to the victim. Not all institutions will launch an investigation after a claim of fraud. Some institutions will not even talk to the victim because there is a bill collection process in place. They repeatedly send the

victim to the bill collector for recourse. Some victims have the bad luck of having a provider commit the crime. This happened in the Skodnek case in Boston. When the original provider commits the crime, there may be no way to get corrections. When that record reaches secondary institutions, correction becomes a nightmare scenario for victims. How do we respond to this aspect of medical identity theft?

This national process needs to be led by this group. You are the professionals trained to handle the complexities of health care records. You are in the unenviable position of being on the front line when a patient or a physician figures out that something is wrong with a record affected by fraudulent activity. So one of my key requests is that you gather the stakeholders together and create a process to respond to the day- to- day problems of medical identity theft.

The second response is Red Flag alerts. Red flag alerts in the financial context are already the subject of regulation by the Federal Trade Commission. These alerts make financial institutions affirmatively react to the potential presence of fraud in order to protect consumers and themselves. Financial fraud red flag alerts have applicability to medical identity theft. In the medical identity theft context, a red flag alert would be placed in a victim's health care file to alert providers and insurers of potential fraudulent activity.

There is no reason the health care sector cannot -- on its own -- create red flag guidelines for use in the medical identity theft context. In the health care sector, software programs already allow various kinds of flagging for health care files. For example, two individuals with the same names who are on the same floor of a hospital often receive a flag or alert in their file. With the common last name of Dixon, I have seen my own family members get just this kind of alert during hospital stays. A red flag dropped into a victim's file and paid attention to by the right people could be a crucial tool for preventing harm for victims, and could be a tool to prevent harm to institutions as well.

The third response is a John or Jane Doe file extraction. Most of you will be familiar with how this works already. A victim tells the health care provider that she is a victim of medical identity theft. In the best-case scenario, the provider will investigate and give the victim the benefit of the doubt. If fraud can be substantiated, then the victim's file is purged of all information that was entered as a result of the fraud. Sometimes, this may be part of the file, in some cases the entire file may belong to the thief. If the thief is unknown, the fraudulent information is completely removed from the victims' file and held separately so there is no danger of mis-treatment due to factual error in the file. That separate file is the Jane or John Doe file. The victim’s file and the extracted file are cross-referenced. This is an elegant solution to a challenging crime, and this solution has many variations. The bottom line is that the bad information is gone from the victim file, and there is a retraceable data trail for any audits.

The fourth response is to have dedicated personnel trained to respond to this crime at each facility. Small providers can have dedicated regional personnel to help. This is a simple response: designate someone as the human interface for victims of this crime. It is in the provider's best interest to resolve this crime, and it is in the patients' best interest to

be able to actually talk to a person about what has happened. This becomes more of a challenge if there is not a process for dealing with medical identity theft in place at each institutional provider, and if there is not a designated person trained in the complexities of this crime to lead this effort.

The fifth response is to focus on the right approach. For example, patient identity proofing to prevent medical identity theft is overhyped. Medical identity theft is primarily an insider crime, not an outsider crime. We hear over and over from vendors and others that the solution to medical identity theft is to check the identity of patients. Well, tell that to the one thousand-plus victims of Isis Machado, a Cleveland Clinic front desk office coordinator who stole identities of patients and sold them. If the Cleveland Clinic had checked each of those thousand patients' identities, it would not have stopped that crime. In fact, as a front desk coordinator, Isis Machado may well have been the one to check identities if such a system were in place.

When I began researching medical identity theft in early 2005, there were no scholarly research studies or even articles on this crime. I had to start from scratch, using existing health care fraud research and prosecution information as well as conducting extensive interviews with institutional providers and law enforcement professionals. One of the first cases I found was that of a gentleman living in Pennsylvania who, much to his surprise, discovered that a man had received 5 surgeries across multiple states in his name. This is a case that exemplifies what I call "one off" medical identity theft, where a single individual steals an identity to get surgeries or prescriptions.

However, after even a moderate amount of research, it became apparent that most medical identity theft was not of the "one-off" variety. Currently, we are well into research for a second report, and we are finding that the preponderance of medical identity theft occurs through a more organized, insider method. ID checks won't help here.

The sixth response is one that should already be in place, that is, risk assessments that specifically include assessment for medical identity theft issues. Risk assessments should be primarily focused on the insider threat scenario, versus the patient threat scenario.

The seventh response is to create training materials to educate the health care sector generally. This effort should ideally be undertaken by a leadership organization with in-depth understanding of health care information flows, and that would be AHIMA. This ties back to the first response, which is to create a set of standards for how to deal with this problem.

The eighth response is education for patients. The World Privacy Forum is doing as much as we possibly can to educate patients about this crime, but we are small and resource-limited. We see some others making efforts to educate victims about this crime. Insurance companies have done a little bit, and we are beginning to see more of this as time goes on. We hope providers begin educating patients about this, too.

We know that medical identity theft exists. We see signs that it is becoming a bigger problem. We are starting to see legislative response bubbling up in this area. In California, the first medical identity theft bill has already made its way through the state senate. If the history of what happened with financial identity theft is any indication, there may be dozens of laws coming forward in this area. Historically, we get legislation when a community does not handle its own problems. That's why we have literally hundreds of financial identity theft laws. The harms to consumers were great, there was inaction in the financial sector, and there had to be a response. Here, we see an almost exact parallel to those early days of financial identity theft. If I were managing health records, I know that I would not welcome hundreds of potentially uncoordinated legislative requirements. This is the right time to take action and to respond to the issues of medical identity theft before others step in and mandate responses you may not like.

I believe we can address many of the key problems medical identity theft causes in the lives of individuals. I ask you to work together to help these victims. We cannot stop the crime from happening just by checking patient IDs. We've seen that this is an insider crime and that prevention will require much more complex and sophisticated responses.

What you as health information management professionals can do is work to create a nationally accepted process for dealing with the aftermath of this crime not just for the institutions, but for dealing with the aftermath of the crime from the individual victims' perspective. Your efforts have the potential to greatly reduce the harms victims experience as a result of this crime.

I have great hope that you can and will do this, and I and the World Privacy Forum will do whatever we can to work with you.

Thank you, and I welcome any questions you may have.