Testimony of Pam Dixon
Executive Director, World Privacy Forum

before

Health and Human Services, American Health Information Community,
Confidentiality, Privacy & Security Workgroup

Friday, September 29, 2006

Hubert H. Humphrey Building
200 Independence Ave., SW, Room 800
Washington, DC 20201

Thank you for your invitation to testify before the committee today. The World Privacy Forum is a non-profit, non-partisan public interest research group focused on conducting in-depth research in the area of privacy. I am the World Privacy Forum's founder and executive director. On May 3 2006, the World Privacy Forum published the first major report on the issue of medical identity theft. The report is a detailed accounting of what medical identity theft is, how it happens, what harms it creates, why it is happening, and what is facilitating it. The report is available on the World Privacy Forum website, as are detailed documents that analyze HIPAA in relationship to medical identity theft.[1]

A short note before I begin: due to the length limitations imposed on this testimony, I was not able to provide detailed corroborating and substantiating information in this testimony. Therefore, I encourage interested parties to look at the report, because it contains numerous substantiating details. The space allotment also left me without adequate room to offer detailed technical explanations and substantiation for my viewpoints. I will be happy to provide these details upon request.

In this testimony, I will lay a foundation for an exploration of identity proofing by first discussing medical identity theft and trust architectures. Then I will focus on identity proofing in the digital environment.

[1] <http://www.worldprivacyforum.org/medicalidentitytheft.html>.

Medical Identity Theft: Why This Crime Cannot Be Ignored in Identity Proofing

Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information -- without the person’s knowledge or consent to obtain medical services or goods, or uses the person’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.

These false entries in victims’ records may be found at hospitals, doctors' offices, pharmacies and insurance companies. Sometimes the changes are put in files intentionally; sometimes the changes are secondary consequences of the theft. The changes made to victims’ medical files and histories can remain for years, and may not ever be corrected or even discovered.

Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them. It is nightmarish that patients’ medical records may include information about individuals who have stolen their identities for the purposes of using the victims’ insurance or for dodging medical bills. However, there is unambiguous evidence that this is already occurring.

As the health care system transitions from paper-based to electronic, this crime may become easier to commit. While it was not possible for one individual to cart around one million medical files in their arms 30 years ago, today, it is a likelihood in a digital environment. Today’s systems allow for not just networking, but the ability to store millions of files on laptops, iPods, and other portable storage devices. The combination of the miniaturization of the health record with vulnerable networks of data that criminals find valuable is at the heart of why medical identity theft is proliferating in the current environment.

After the crime has been committed, victims may find it more difficult to recover from medical identity theft as medical errors are disseminated and redisseminated through computer networks and other medical information-sharing pathways. There are additional issues that provide barriers to recovery, but that is not the focus of this testimony.

Medical identity theft is largely a crime that is perpetrated by trusted insiders, with organized crime exerting a strong influence on this particular crime. While there are individual cases of medical identity theft, for example, where one person steals one identity and gets surgeries or care in a victim's name, the majority of the harm from medical identity theft does not arise from these individual cases but from cases involving trusted insiders working to scale using the identities of dozens or even thousands of victims and coordinating their efforts with crime rings.

For example, doctors are trusted insiders. So are billing clerks, nurses, and others. Because they are trusted insiders, these individuals have access to patient records, many times appropriately so. Access to patient records can be accomplished rapidly and on a large scale today, which means big incentives for inappropriate access and ultimately large cash payouts for crime. When a trusted insider is the proverbial rotten apple in the barrel, this can and has resulted in large identity theft rings operating out of hospitals and clinics. This is a source of harm to the system, and introduces identity and accuracy problems into patient records.

Medical identity theft is a substantial risk factor in the healthcare world, particularly for institutional providers who typically maintain large quantities of digitized patient information, which is a lure to criminals seeking to capitalize on the data. It is important to frame the issue of medical identity theft correctly so that the current and future risks to public safety, health record accuracy, and medical research quality can be addressed correctly. This is a fundamental problem facing the medical sector, and it needs to be recognized and acted on in appropriate and effective ways. There are answers to help resolve these challenges, but to do so, the fundamental architecture of the healthcare system must be understood.

The Trust Architecture

The architecture of medical sector data flows has historically been based in large part on the old paper-based billing and treatment system. This old system was built on the concept of trust, that is, "I trust you to be who you say you are." Trust takes on various forms and architectures in our modern world, including something called “transitive trust” systems. But at its core, medical sector systems are by and large still trust-based systems, no matter how many new names the technologies have. While the current-day payment/treatment system contains many differences from systems in place 25 years ago, the current system is still essentially architected on a trust model.

One can speculate that perhaps this model may have been able to keep up if the current round of ambitious modernizing and networking projects had not been overlaid on top of it. But the reality is that the current medical sector data architecture now allows treatment and payment systems to be networked across states and across the nation, sometimes in near-real time. Tens of thousand of institutions and millions of individuals have access to patient data from many multiples of data points, for purposes of both observing and changing the data. Many have expounded on why there is benefit to networking an individual’s health record, and there may indeed be benefit. But in terms of identity, this kind of high-activity overlay onto the old system also poses substantial risks.

The Merging of Payment and Benefits in a Digital Environment

In the paper-based world, payment and treatment systems were largely separate, and the two did not commingle any more than necessary to process payments. But in the digital, networked world, these systems are for all intents and purposes identical. And in practice today, these systems are increasingly being merged.

Perhaps the most obvious example of this process are the projects well underway in California, Tennessee, and elsewhere that use insurance billing information as a proxy for the electronic health record of patients. The way this works, broadly speaking, is that a patient shows up at an institutional provider without a record being held by the provider. The provider queries insurance company records, and the insurance treatment/billing codes are used to populate the electronic health record fields. So a person who filed a claim for treatment of a broken arm will have a broken arm code put into the treatment fields of the patient record. CalRHIO currently has an Emergency Department Information Linking pilot project that will use a Blue/Cross Blue/Shield insurance information set as a foundation of part of the patient emergency room record for those who do not have a health record on file with the provider. The linking is in the process of being set up across selected providers in California.[2]

In a perfect world, this could be a great idea. Patients without records will get them. But in the real world, fraud is rampant, and that changes the outlook for this kind of activity. Health care fraud accounts for an estimated 3 to 10 percent of all health care costs, or 80 to 120 billion dollars of loss per year.[3] If even the lowest estimate of healthcare fraud is correct, then potentially millions of patient files stand to contain errors that are distributed and redistributed through the system. An error in one insurance file could cause the death of an identity theft victim who presents in an emergency room that allows population of patient files with insurance files.

While HHS and AHIC have been promoting electronic health records, victims of medical identity theft and the impact of healthcare fraud on proposed systems have not had a voice. It is unreasonable to insist that the medical sector never be digitized. However, there is a correct process for doing so, and it is just as unreasonable to avoid appropriate

[2] <http://www.calrhio.org> See Emergency Department Information Linking project.

[3] Government Accountability Office, May 7, 1992. T-HRD-92-29. Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse. Statement of Janet L. Shikles, Director, Health Financing and Policy Issues, Human Resources Division. “Though no one knows for sure, health industry officials estimate that fraud and abuse contribute to some 10 percent of U.S. health care's current $700-plus billion in costs,” p. 2.

risk assessment and mitigation in all projects and plans, including current pilot projects such as the emergency department linking pilot project in California. To date, the process of architecting pilot projects have not been undertaken with acknowledgements of risk factors such as medical identity theft. If HHS continues to guide this process in the current manner, then a series of unpleasant and unnecessary negative consequences may well ensue, including the injury or death of patients because of the sharing of incorrect information through pilot or established networks.

Some may say that audit trails will solve problems of inappropriate access of digitized data by insiders, and inappropriate use of or additions to patient records. But audit trails required today by HIPAA are incomplete. Clever insiders can alter audit trails. More importantly, the resources available to review audit trails are nil, and problems will only be found after patients have been harmed. The fundamental architecture is flawed, and an audit trail won't fix this. Audits trails will also not resolve errors within health records.

Patient Identity Proofing in a Digital Environment

If audit trails are not the answer, does identity proofing provide an answer to some of these issues?

Several overriding concepts here are crucial.

First, the most perfect patient authentication system in the world in any context will not resolve the issue of identity theft in the medical context. Patients could be identified to a near certainty if not certainty, and yet an estimated 85 percent of the medical identity theft problem in healthcare provider settings will remain unsolved **because the majority of medical identity theft is committed by trusted insiders**, not by the patients. If a provider is using a trust architecture, and there has been a fundamental breach of that architecture, identity proofing will do little good. The best short and non-technical example of why patient identity proofing is not the solution is to look at the current situation in the financial sector. To crack the current identity systems in place, an identity thief has to produce foundational identity documents such as a fake driver's license, or so on. After the foundational identity documents are compromised, the architecture of trust lets the thief run rampant. There is already a case where this has happened to an institutional health care provider, which is discussed in the Forum's report.

Second, if underlying architectural problems are unaddressed, then the solutions resting on top of those architectures cannot work as well as they need to. As an example, some hospitals have turned to a "TSA style" of identity proofing requirement before allowing treatment of patients. Hospitals using this sort of a system, and their number is growing, require patients to show a photo ID. This ID is photocopied and added permanently to patients' medical charts. In some hospitals, this process is digitized, so drivers' licenses and other identity documents became a permanent digital part of the patient record. Hospitals across the nation are discussing moving to this sort of system.

This is not the right answer. If put in place, these practices will greatly increase patient risk of harm. Now, instead of just getting a medical file when there is a security breach, criminals will get digital photographs, digital copies of the drivers' licenses, and other robust identity proofing documents to work with as they themselves attempt to impersonate others. This is the double edged sword of trying to proof identity: as you collect documents to proof identity, you put the data subject in a position of increased risk if the documents are leaked. This is a well-known phenomenon in the financial sector. Meanwhile, the smart criminals simply show up with a matching set of fake ID documents.

It is important to keep in mind that identity proofing documents are compelling data sources and are likely to suffer a security breach, just as standard health records suffer from being breached today. As we have seen in the past two years since state-level data breach notification laws have come into effect, health care providers are the source of some significant and potentially dangerous data breaches. If robust identity documents are added to patient medical files, then when those files are stolen or breached, there is the potential that more harm will be and can be done to patients.

Third, in working to genuinely authenticate identity, one must typically utilize various well-tested information verification schemes that are common in the financial sector. Many such schemes exist, usually involving the incorporation of multiple data points, tiered access schemes, and so on. In bringing this style and this kind of process of authentication into the medical sector, vulnerabilities on a scale that we have not seen before are introduced. The potential for short and long term harm is real and it is significant.

The financial sector uses tools such as credit reports as well as anti-fraud and identity products such as those from Fair Isaac and others. The financial sector also uses near-real time Social Security Number authentication, as do many retail employers during job application processes. This kind of information is highly regulated in its use, and falls under the Fair Credit Reporting Act (FCRA) when it is used for making determinations about an individual's creditworthiness, for example.

But these same kinds of tools, if used by health care providers, will not necessarily always covered under the regulatory framework of the FCRA, and this could pose substantial patient risk and harm issues over the long term that many providers may not have considered or fully understand. The FCRA gives data subjects important rights and remedies, for example, the right to correct errors in a credit report. There are no parallels to the FCRA under **HIPAA, which does absolutely nothing to protect the abuse of this sort of information**.

Fourth, financial systems generally have a different access architecture than medical sector systems. The underlying ideas of access and the fundamental architecture are different. Access to internal banking systems is tightly controlled, as it should be. The medical world is completely different, because access cannot be tightly controlled in some medical settings, particularly where speed of access by multiple healthcare experts is an issue. Because of this and other factors, much of the medical information environment is like an information sieve with many data access points. Adding networked access of patient information on top of this scenario serves to multiply the challenges a thousand fold.

What to Focus On

Going forward, it will be crucial to find appropriate balances to identity proofing. It is perfectly acceptable to ask a patient to see their identification. But it is not acceptable to add that detailed information to a patients health record, because of risk factors and factors due to potential abuse of the information for secondary or other purposes. It is perfectly acceptable to work with digital signatures to assure certain aspects of security. But it is not a fix to rely on digital signatures to resolve medical identity theft when thieves are operating from the inside. There are many options to pursue here, but if they do not address the underlying architectural issues and challenges, then these issues will continue to remain troublesome and may ultimately cause a loss of trust in networked systems.

This committee is focusing on methods to verify patient identities in various situations. That may be a part of the solution, but adding data brokers, credit bureaus, SSN authentication, and other financial system methods to the health sector will likely make things worse. These methods have not stopped financial identity theft. It just produces smarter crooks. Industry doesn't much care as long as its financial losses are low. Indeed, legitimate financial institutions profit from identity theft by selling potential victims identity theft insurance and credit monitoring. That attitude will not work for the health sector.

Instead of focusing on "identity proofing" patients, HHS needs to focus on identity proofing trusted insiders. Instead of focusing on finding ways to prove patient identity, HHS should be finding ways to allow patients to access and amend their health records. Technically, HIPAA allows a right of access and amendment, but the rights are limited. Victims of medical identity theft are often not allowed to see or correct their records. Victims need real rights, and health care institutions must accept responsibility for their errors. If a health data network allows everyone to pass the buck to someone else, then that is the wrong network.

Instead of focusing on proofing the patient, HHS should also be looking at the existing fraud in electronic systems and at the ways false billing and treatment information in digital systems stands to harm human health. Not only does fraudulent information that is perpetuated and multiplied in electronic systems harm individual health, it also harms public health, and medical research that relies on the records. No one has any idea if records research studies report false results because some of the data comes from records of identity theft victims.

AHIC should take a long, sober look at its projects and plans. It should undertake thorough and realistic risk assessments, and it should be at least open to the idea that its plans and projects may not be in the best interest of patients' well-being unless the challenges and problems that medical identity theft and other forms of fraud are acknowledged and fully resolved. A health network that harms patients and propagates fraud is not what we need. We should not repeat the mistakes in the financial system that led to the rise of identity theft in the first place.

I urge the committee to pay attention to health care insiders as well as on patients. If you do decide to go forward with financial sector style screening, then you should be including standards and procedures that mirror the financial sector legislation designed to ensure robust transparency, recourse, accountability, and adequate and responsible risk assessment. Note, however, that the financial sector legislation is not perfect, does not stop identity theft, and gives data subject inadequate rights and remedies. Health care must be held to a higher standard because mistakes mean that people will die.

In closing, I ask you to thoughtfully and soberly consider the risks to patient health through data inaccuracy that medical identity theft and its associated crimes brings into the medical sector. I ask you to look at current NHIN and other pilot projects and work to fraud proof them and find ways to ensure accuracy of patient data. It is tempting to talk about PKI and transient trust and other glitzy technologies. It is tempting to look at the financial sector and think you can simply take their tools and apply them to the medical sector. But I want to remind you as clearly as I can that for a patient who has had his or her medical identity stolen, and whose medical file and insurance record has been changed as a result, the problems cannot be solved by even perfect patient identity proofing.

Respectfully submitted,

Pam Dixon