Testimony of Pam Dixon
Executive Director, World Privacy Forum

Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments

Before The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality

San Francisco, California

Tuesday, August 16, 2005

Chairman Rothstein and Members of the Committee, thank you for the opportunity to testify on issues of privacy and confidentiality as they apply to Electronic Health Records (EHRs) and the National Health Information Network (NHIN). My name is Pam Dixon and I am the executive director of the World Privacy Forum. Founded in 2003, the World Privacy Forum is a non-profit, non-partisan public interest research center. Our work focuses on in-depth research and analysis of technologies and their impact on society, with a particular view to the privacy and security implications of emerging technologies and data infrastructures.

The World Privacy Forum has been particularly interested in developments related to EHRs and the NHIN. Given the impetus of the 2004 Executive Order [1] mandating forward movement in these areas, and the broad impact digitized medical records will potentially have on patients and on the healthcare sector, the World Privacy Forum believes that the decisions this Committee and others shaping these efforts arrive at will be of lasting importance. Given the transition of many parts of our society from analog to digital, it is crucial to ask what this digitization will look like and to carefully examine and discuss what form EHRs and related systems should take in regards to patient choice, privacy, and security.

In February of this year, the World Privacy Forum and the Electronic Frontier Foundation submitted joint comments in response to the Request for Information on the NHIN. Our comments focused on the privacy and security implications of the NHIN.[2] Since that time, the World Privacy Forum's efforts in this area to date has been to conduct research on the uses of new technologies in hospital settings, such as the uses of RFID, and to

research the issues of patient choice, privacy, and security and how those issues relate to EHRs and to a networked environment on a variety of scales, from intimate to large. This is the kind of work the Forum likes to focus on; we have conducted previous studies of networked data flows; our year-long, sector-wide 2003 study of employment data in networked environments is an example of this. [3]

The digitization of health records and the challenge of creating a secure networked structure to house EHRs and other data flows brings forward many complex issues. The first issue I will focus on today is that of patient choice as it relates to EHRs and their transmission and storage. I will then discuss some specific questions about the NHIN and its cost and security factors. I will conclude with ten proposed questions that I believe will be crucially important to consider as the planning and implementation of EHRs and the NHIN moves forward, and the set of Fair Information Practices that I believe must inform these efforts.

I. The Core Role of Patient Choice in Electronic Health Records and EHR-Related Systems

Electronic health records do not exist within a vacuum. Like paper medical files, EHRs must be stored somewhere. And in order to be used and compiled, the records must be accessed in some manner. Unlike paper medical files with their unique set of physical controls which have inadvertently slowed dissemination (often called "privacy through obscurity"), EHRs are prone to rapid dissemination and can be called up from multiple access points simultaneously.

Because of the substantial changes that digitization of EHRs and other medical data brings, patient choice in the realm of digitized medical data will be a core issue that this Committee must grapple with. It is in this area that the strengths and weaknesses of any EHR system, large or small, networked or not, become evident. Patient choice becomes particularly important, for example, in light of medical identity theft and medical security breaches. It is these and other specific patient choice issues to which I will now turn my attention.

A. *Identity Theft and Electronic Health Records: The Centrality of Accuracy, Access, and Right of Correction*

In addition to impacting financial issues such as credit reports and credit cards, identity theft also impacts individuals' medical lives and their medical records. It is perhaps the ultimate invasion of privacy to have one's medical records and information stolen and used by another. Sophisticated bad actors are increasingly stealing identities for the specific purpose of obtaining medical treatment, or to obtain prescriptions or medical devices for resale. This is not a scenario that is far off in the distance, it is happening right now, and it will have a profound impact on privacy, confidentiality, the accuracy of medical records, and on how healthcare providers authenticate the identity of individuals.

This is especially true in the case of EHRs, which are being touted as life savers due to increased accuracy by way of being digitized. Medical identity theft unfortunately may lead to the alteration of medical files, as seen below. This fact throws the idea of increased accuracy into doubt for those who are victims of this emerging medical information crime. Digitization may in fact serve to exacerbate this problem, not solve it, particularly in the case of records that are networked.

Note these recent examples of this problem:

- July 26 2005, Pennsylvania Attorney General Tom Corbett announced an action against a 51 year-old Philadelphia man who used another individual's name and health insurance information to obtain medical care at five different hospitals in Philadelphia and in New Jersey. The medical identity thief raked in over $144,000 by repeatedly using this individual's name and medical insurance information without that person's knowledge or permission. The identity thief's hospital bills were submitted to Aetna Insurance, which paid $56,230 in claims before halting payments. [4]

- July 15 2005, a Lufkin, Texas identity theft victim received someone else's medical bills after that individual used the Texas man's identity to get medical treatment. The only tipoff the victim received about the problem was the bill after the fact. [5]

- In California, unscrupulous medical providers were buying Medi-Cal and Medicare patient identity numbers and were using them to get reimbursed for millions of dollars in tests and other services that were never provided. Of $34 billion annually spent by the Medi-Cal program for health care for approximately 7 million Californians, state officials estimate that as much as $14 billion of that amount is stolen in similar fraudulent scenarios. [6]

  The California Medi-Cal identity theft scam specifically involved bad actors using stolen patient information purchased for as little as $100. During interrogations, investigators learned that workers in medical records offices and billing departments had copied the information for cash. Investigators said *searches have turned up medical charts in the process of being altered*, with some that are postdated or written up in a way that makes no sense. [Italics added].

- August 5 2005, a Canadian man impersonated his bother to receive medical services in the Toronto area. The investigation revealed that a man was found to have assumed his brother's identity and had gone so far as to receive an Ontario Health Card in his brother's name. The Ontario Health Card was then used to access health care services between 1999 and 2002 under the false name. During this time period the accused had an Ontario Health Card in his real identity and was eligible for insured health care services. [7]

Of particular note is how identity thieves may intentionally alter or inadvertently cause to be altered victims' medical files to reflect diseases or a medical history that the victim likely does not have. It is nightmarish that an individual may have the medical chart of someone who has stolen his or her identity, but it is a factor that must be taken into account at this point, and one that must be countered preventively. If medical identity theft is not taken into consideration in the management and design of EHRs, then instead of promoting health record accuracy, EHRs of identity theft victims could inadvertently prove to be damaging or even deadly to those patients. It should not be an expectation that all or even most victims of identity theft will learn of their problems prior to presenting to a physician.

This is not a hopeless situation. While identity theft is certainly problematic for any EHR system, whether paper or electronic, the architecture of a digitized EHR system can be built in such a way so as to make checks and balances on data accuracy an integral part of the system. Given that the implementation of EHR –based systems has not reached critical mass yet, now is the right time to mitigate the specific risks of inaccuracy of medical data due to medical identity theft. The Centers for Disease Control and Prevention have reported that less than 20 percent of physician practices now deploy clinical IT systems that track a patient's medical history, including lab tests and medications. A GAO report cites adoption rates for fully operational EHRs as 31percent for physician group practices and 19 percent for hospitals.[8]

The specific risk for an EHR system in the case of medical identity theft, beyond accuracy, is the rapid dissemination of the EHR within a networked setting. Great care needs to be given to the electronic data file and all of its components such as X-rays, lab tests, and so on to determine prior to any networked dissemination if all of that data belongs to the patient. It is in the patient care setting that the correction of an EHR is most likely to take place, so it is logical that prevention efforts would be focused in this area.

Now is also the right time to start thinking about changes that could be made to HIPAA to give patients the right to correct entries made to their medical files, including those made by third parties outside the patient care context. Allowing patients to correct their records and entire medical file will specifically address the problematic accuracy issues raised by identity theft as applied to medical records. And again, to reiterate, now is the right time to build baseline EHR architectures that accommodate such correction and patient choice.

Medical identity theft is increasingly a sophisticated, organized operation that will require a good deal of time and attention to combat, and it is an issue that will impact any networked system involving EHRs.

B. *Patient Choice Regarding Participation: Can A Patient Opt-Out of the Digital Environment? If so, who gets to opt out?*

One of the fundamental decisions that must be made about the use of EHRs in various environments, particularly the NHIN, is whether or not patients will be allowed to have the choice of opting out of the system.

An opt out could take a number of forms. For example, a patient could be treated and his or her information could be put into an EHR format. That patient could then choose whether or not that EHR became part of a larger regional or national health network. Or, that patient could decide whether that EHR could be used for medical research. Or perhaps the patient could opt out of having an electronic record at all due to the security risks involved and decide to use a paper record instead. Certainly, allowing patients to opt-out of having their records enter a larger network will be an important right to confer going forward.

In thinking about EHRs and the NHIN, it is useful to remember that in a digital environment, a health record of a public official such as a member of Congress or a law enforcement professional could be accessed from multiple points by any number of people, bringing confidentiality questions into sharp relief. Even if there are barriers to entry to the system, there will inevitably always be one bad actor who has legitimate access and who will not care about the consequences of misusing a medical file. The security and access considerations of medical records are a profound point to consider, as I will discuss later in this testimony. Because of the risks and the confidentiality issues, it would be surprising if there were a complete absence of requests for opting out of the system.

The question of who gets to opt out of the system, if anyone, is a challenging one. If for example, only members of Congress, public figures, and law enforcement officials are allowed to opt-out of the NHIN or even an electronic format for medical information, how will this be explained to the public, and when? What recourse would members of the general public have for being considered for "opt-out eligibility?" Would, for example, victims of domestic violence receive special consideration?

Some have noted that no one should be able to opt out of any future NHIN or EHR system. This is not an option I endorse. If this option is pursued by the Committee, however, examining how security will be handled so that risk of breach and misuse is greatly minimized will become a key burden. Also important will be allowing patients to electronically track the transactional record of who has accessed their EHR in real time so as to enable patients to protect themselves from misuse of their information retroactively if necessary.

The issue of opt-out creates stubborn questions, and I believe these are precisely the questions that must be addressed robustly and publicly prior to the implementation of any NHIN, or even prior to requiring patients to have their medical information stored in EHRs.

C. *Blanket Consent in a Digital Environment*

Given the ease of distribution of EHRs and the attendant privacy implications, it is probable that single-request, blanket patient consent will no longer be appropriate in such a system. If for example, a patient gives consent for one-time use of an EHR in a single hospital, and the EHR is then uploaded into a regional health network, does that same consent then apply to the broader system? I do not think that it necessarily does.

In an electronically mediated health records system, revocable, reviewable consent architectures may be built into the system from the outset. In such a system, patients would have the right to review the "e-dissemination record" of their EHR data flows and make decisions about granting or withdrawing consent based on what they have seen.

Patient representatives could be appointed at key junctures throughout the medical infrastructure to attend to patient questions and concerns. There should be serious consideration given to the idea that due to the risks of misuse of patient data, patients should have a private right of action when their data – or consent – is abused.

Concerns about consent in EHRs or networks involving EHRs is not an academic point. Patient consent in electronic environments is already an issue, however it is being ignored in practice. For example, the Wall Street Journal reported that several New York City metropolitan-area hospitals – including NYU Medical Center -- are currently working on a pilot program to give emergency rooms access to information about patients treated at other regional hospitals, with a timeline of two years to implementation. [9] It is unknown if the entities involved will seek additional patient consent for the use and transmission of the data. It is also unknown if the privacy policies of the entities will be updated to reflect these new uses, and it is unknown if patients are being given the right to opt-out of this system.

An article about "Disaster-proofing your EHR" [10] noted that a third-party, Web- based EHR pilot program in use by a Toledo physician and 15 others across the nation was the answer to natural calamities. The project used remote servers to reduce costs for the doctors and to "ensure data safety." The program may sound good, but the result of the program was that patient data was going to a third party server apparently via the Internet and was under the control of third parties. Were patients informed of this data transfer? Did they consent to this data transfer? There are also acute computer security questions that would need to be asked in any audit of this system.

Similar demonstration projects are proliferating. The Doctor's Office Quality Information Technology project, funded by the Centers for Medicare and Medicaid Services will operate 2-year projects in five states to support primary care practices in adopting EHR and collecting information on quality of care.[11] Another EHR system pilot project sponsored by the U.S. Centers for Medicare & Medicaid Services will be tested in small-to-medium sized physician offices in California, Arkansas, Massachusetts, and Utah. In California, there are at least 150 to 200 physicians across the state participating in the project. [12]

While these examples of demonstration projects and pilot programs are positive in

showing forward momentum in technology adoption, they also reveal that EHRs are being used with real patient data without a standardized policy infrastructure to support their use.

An established model of patient consent in an EHR setting would aid patients and physicians in determining where the boundaries of consent are. And this structure needs to be robust, revocable by the patient, and put in place prior to any use of data.

D. Security Breaches in the Digital Medical Environment

From January 1 to August 15, 2005, there have been 94 known security breaches impacting potentially 56 million individuals. So far, many of the breaches have affected financial information, but 12 of the breaches have been specifically of medical-related information.

- 01/05 **Christus St. Joseph Hospital, Houston Texas: 16,000 individuals**
  - News reports published in April noted that the hospital sent letters to 16,000 patients saying their medical records and SSNs may have been compromised due to the theft of a computer in a January burglary. The stolen machine was one of two computers taken from Gateway File Systems Inc. Gateway was converting paper medical records to digital files for the hospital. [13]

- 01/05 **Kaiser Permanente: 140 individuals**
  - Kaiser notified patients in March 2005 that a disgruntled former employee calling herself the "Diva of Disgruntled" had posted confidential information about patients on her Weblog. The information included medical record numbers, patient names and in some cases information about, but not results of, routine lab tests. The U.S. Office of Civil Rights discovered the breach in January. The material, posted in January, was only taken down from the Web in March, whereupon the employee reposted it again and the hospital had to take it down a second time. The California Department of Managed Health Care fined Kaiser Foundation Health Plan Inc., a division of Kaiser Permanente, $200,000 for the breach. [14]

- 03/28/05 **San Jose Medical Group: 185,000 individuals**
  - Two computers containing patient billing information, including names, addresses, and Social Security numbers were stolen. [15]

- 03/28/05 **University of Chicago Hospital: 85 individuals**
  - The hospital announced that an employee had been using credit card information from patient records. [16]

- 04/15/05 **California Department of Health Services: 21,600 individuals**
  - The CDHS confirmed the theft of a laptop computer that contained personal information May 26. Names, SSNs, and health information for 21,600 recipients of Medi-Cal services was on the laptop. The computer was stolen from the locked trunk of a car of an employee of a company that provides data services to the state.[17]

- 05/26/05 **Duke University Medical Center: 14,000 individuals**
  - Duke notified patients that a hacker broke into its computer system and stole 5,500 users' passwords and nearly 9,000 fragments of Social Security numbers belonging to medical school alumni, medical center staff, faculty and trainees. [18]

- 06/30/05 **Ohio State University Medical Center: 15,000 individuals**
  - Confirms notifications to patients whose billing information was contained on a laptop computer stolen from MTE Consulting's office in April. [19]

- 07/ 05 **Colorado University, Boulder Health Center**: **42,000 individuals**
  - Names, SSNs, addresses, dates of birth of 42,000 individuals, plus about 2,000 lab test results were stolen by a hacker who broke into the health center servers. [20]

- 07/13/05 **Blue Cross Blue Shield of Arizona : 57,000 individuals**
  - The company confirmed theft of backup tapes that contained policyholders' addresses, phone numbers, Social Security numbers and dates of birth. The tapes also contained partial treatment histories for some patients and certain information about the doctors who provided that care. [21]

- 07/25/05 **St. John's Regional Medical Center, Joplin, Mo. : 27,000 individuals**
  - Acknowledged the theft of two computers containing patients' names, dates of birth and some medical account numbers. The computers were stolen from KC & Associates, a company that at the time converted the hospital's patient records to microfilm for easier storage. [22]

- 08/01/2005 **University of Florida Health Science Center (ChartOne): 3,851 individuals.**
  - At least 3,851 patients of University of Florida physicians were notified they were at risk for identity theft when a laptop containing their names, Social Security numbers, dates of birth

and medical record numbers was stolen from a subcontractor's office. [23]

It is important to remember that these data breaches have occurred within an environment which is only partially digitized, that is, not every hospital has an EHR/IT system and not every hospital is part of a regional or even city-wide networked hub. It is unlikely that the breaches will slow down when EHRs become prevalent, in fact, it is probable that the opposite will occur. The question of security breaches will thus become an increasingly crucial one for the Committee to address as EHRs become adopted and exchanged over various networks.

I will touch on specific security risks in networked environments later on. Here, I would like to note that security breaches will be part of any digital medical environment because the current medical system is architected in such a way that breaches are inevitable. Fundamentally, the modern health care system is an open-loop system, with a closed-system being the exception rather than the rule.

The healthcare system provides information to a wide range of users through a complex series of dataflows, and that is not likely to change. Primary users include information flows to caregivers and their support system, for example, pharmacies and clinical laboratories. Secondary users include payors, insurers, government benefit agencies, accrediting organizations, bureaus of vital statistics and health departments, scientific researchers, as well as marketing firms and vendors of health-related products. [24]

Given these substantial data flows and all of the increased risks these flows bring, the loss of privacy and confidentiality due to security breaches will have to be part of the Committee's planning as it considers the NHIN and even the structure of individual EHRs. Going forward, it will useful to consider industry-wide standards and regulations governing breaches. These regulations would ideally include patient notification and private right of action.

Because security breaches are a question of "when" not "if", it will also be of great value to set up regulations beyond HIPAA that discuss how to store patient medical data within EHRs, in other words, to focus on what can be done in the area of prevention. To cite a few examples: truncation of SSN, disaggregation of personally identifiable information with the medical history, and strong encryption of EHRs are among the many steps that could be instituted. Also preventing the datamining and marketing use of the data will be steps that have protective and preventive value. While industry best practices are a beginning, in the area of patient medical data industry best practices should not be relied on as a sole solution.

E. *Patient Trust and Choice*

If (or more accurately, when) patients' information is breached and patients are not able to opt-out or do not have robust fair information rights such as access, correction, purpose

specification, among others, there is a real possibility that patients will cease to trust EHRs and the systems they flow within such as an NHIN.

Additionally, given the number of entities that have access to patient healthcare information under the current iteration of HIPAA, there is possibility of increased misuse of EHR data given the ease of transmission in the digital environment. Such misuses have been documented by the National Academy of Sciences in "For the Record: Protecting Health Information." The report gives an example of discrimination resulting from access to genetic information, such as loss of employment, loss of insurance coverage, or ineligibility for insurance. In some cases, discrimination was based merely on evidence of predisposition to a future occurrence of treatable diseases such as hemochromatosis and Huntington's disease.[25] In an NHIN context, an element such as the personal medical history will provide plenty of fodder for employment discrimination for some patients.

Which brings me to this question: In the situation where patients no longer trust a digital records environment or a system like the NHIN, and they cannot opt out of the digital system, then what quality of medical care will be available to these individuals? There will be individuals, likely those who need healthcare the most, who will simply avoid the medical system and will possibly receive poor healthcare, or perhaps even no healthcare. This scenario should be understood as a real possibility and should be taken into careful consideration when planning especially networked systems.

This is one among many reasons why full patient choice must be built into EHRs in every aspect, and into any networked system such as regional information hubs.

F. *Can a Patient Access and Correct Their Electronic Record? (EHR and Transactional)*

I have discussed inaccuracy of patients' EHRs resulting from identity theft. I realize that further discussion of this point is slightly off-topic, however, to be thorough on this point, I would like to point out that other types of inaccuracies also exist. For example, mixed file inaccuracies can afflict Personal Health Records. And transcription errors do not go away simply because a medical file is in electronic format. While there is a very strong argument that EHRs increase accuracy, it should be remembered that the information from paper medical files has to be entered, often painstakingly, into digital format. This is not always a process that promotes increased accuracy.

For example, a Wall Street Journal reporter relayed the following scenario regarding her personal physicians:

> "When my internist, Michael Palumbo of Manhattan's Murray Hill Medical Group, set up an IT system in 1998 with his 13 partners at the time, they had to type in the necessary information themselves, including prescriptions and ailments for around 15,000 to 20,000 patients. The practice has grown now to around 110,000 patients, but much of the data is now entered incrementally by the physicians as they see patients.

> New York internist Bruce Yaffe installed an IT system three years ago, but it still isn't fully operational because of the mountains of data from 70,000 charts that initially have to be typed into the system. "We couldn't take the time to slow down and implement the electronic medical record. It would have sunk us financially," says Dr. Yaffe, who is also a gastroenterologist. He now has three employees scanning data for about 70 patients a day, prior to their visits. Each chart takes between five and 30 minutes, depending on the size of the file."[26]

Even highly digital systems are not perfect. The inaccuracy of credit reports should be a cautionary red flag. Accurate EHRs, and therefore lifesaving EHRs, depend on accurate typing and on zero scanning errors. And we all know that there is no such thing as hundreds of thousands of perfects scans or an absence of errors in over 70,000 typed-in entries. If this effort the Wall Street Journal reported is expanded to a large scale, you can begin to get an idea of what an extraordinary undertaking the digitization of pre-existing medical files will be on a national level.

For these reasons, and for the reasons I have already mentioned in regards to the impact of medical identity theft, patients must have access and correction rights to their EHRs.

II. The National Health Information Network

To date, there is no firm articulation of what the NHIN will look like. Because of the amorphous nature of the descriptions available of the NHIN, I can only comment on the broadest issues it brings forward. I have already addressed some of the patient choice issues related to the NHIN. Here, I would like to focus on cost and security issues very specifically as they relate to the NHIN.

A. *Cost of the NHIN*

To date, I have not seen a consistent set of firm estimates for what it would take to build and maintain the NHIN. It is reasonable to estimate the cost would rise to at least the tens of billions of dollars, and easily more. One recent study published in the Annals of Internal Medicine noted that the NHIN could potentially cost more than $156 billion in initial capital investment and $48 billion in annual operating costs over the next five years. Ongoing interoperability efforts would cost about $21 billion annually, researchers found. [27]

In the current NHIN plan, statistics supporting the idea that electronic health records potentially could save between $78 billion and $112 billion a year by reducing tests and improving administrative procedures are quoted.[28] A GAO report noted that government estimates of potential nationwide savings resulting from the adoption of health IT is based primarily on two studies conducted by the Center for Information Technology

Leadership. All totaled, there is much discussion of how the NHIN would reduce costs, but the numbers are still in flux. [29]

What will the NHIN cost? What will the cost savings of the NHIN be? And will the cost savings the NHIN produces be enough to cover the actual cost of building it in the first place?

Before cost saving is named as a benefit of NHIN, the actual or anticipated cost of the NHIN should be closely determined as well as any potential cost -savings.

Also, cost-saving methods should be weighed against privacy concerns and ethical considerations. For example, it would generate revenue to allow datamining of EHRs for marketing purposes. However, because of the substantial privacy issues this datamining of the EHR material represents, this should not be considered or allowed, just to name one example.

B. *Privacy and Security of the NHIN and Implications*

I do not doubt that the individuals and agencies involved with the development of the NHIN plan on robust security. However, the security issues that come into question in planning an NHIN of any size or configuration are quite profound. With multiple access points spanning potentially across the nation and through many different institutions (hospitals, physicians in private practice, insurors, payors, government agencies, etc.), the NHIN has the potential to become a medical security fiasco, and therefore a privacy and confidentiality fiasco. Great care must be used in planning any formal or informal system of records due to the clear risks to patient privacy and confidentiality that security breaches represent.

Privacy and security are both, to some degree, matters of economics. Thus, privacy and security countermeasures have historically worked by raising the costs of undesired behavior. The two main complementary strategies are deterrence and prevention, or the imposition of obstacles. Tactics of deterrence include liability or accountability rules that typically look backward. Tactics of prevention include strict access controls, cryptography, and de-identification of individual patients, among others. Because of the highly personal data contained in medical files, any efforts made must tip strongly in favor of prevention, rather than on relying on punishing bad behavior after the fact as a deterrent.

I would like to take just one of these prevention tactics, access control, and use it as an example of the security challenges the NHIN faces. The reason I choose this example is because access control is a central issue any form of an NHIN will have to address.

It stands to reason that the NHIN will put forth a tremendous amount of effort in the area of access controls. Surely, a discussion of multi-level access controls, or tiered access to information will arise in this context. On the surface, multi-level access control sounds

like a reasonable and sound solution to the problem of protecting the privacy and security of patient data.

But the research does not bear out the standard thinking line of thinking on this issue, that it, that tiered access solves this particular security challenge. The National Research Council, in discussing the privacy and security implications of nationwide ID systems is pessimistic about multilevel access controls. The report notes:

> "A further complication would result if it were decided that different users should be granted different levels of access to the database . . . . This raises query capability, access control, and security issues. . . . It is a significant challenge to develop an infrastructure that would allow multiple kinds of queries, differing constraints on queries (based on who was making them), restrictions on the data displayed to what was needed for the particular transaction or interaction, and varying thresholds for security based on the requirements of the user." [30]

The scale of the NHIN means that "if a single identifier is relied on across multiple institutions, its fraudulent or inappropriate use . . . could have far greater ramifications than if used in only a single institution." [31] Thus, "[a] guiding principle in the design or selection of authentication technologies should be to minimize the linking of user information across systems unless the express purpose of the system is to provide such linkage. [32] Moreover, such systems "should be designed to make secondary uses difficult, because such uses often undermine privacy, pose a security risk, create unplanned-for costs, and generate public opposition to the issuer." One of the difficulties here is that the NHIN will be in part designed for secondary information flows, thus greatly complicating access controls.

Another issue with multi-tiered access controls, is that if taken to their logical conclusion in this environment, the system would possibly require a large-scaled, tiered identification scheme apart from, for example, drivers' licenses or standard government-issued identification documents. What entity would administer the medical access/identification scheme? Private companies, or government agencies, or a combination? And what entity would pay for the system, authenticate people to use it, potentially pay for the background checks necessary to gain clearance, and then manage any resulting system of credentials? The U.S. government has an identity card for its employees that would suffice for this purpose, but if a government identity card is chosen as the access mechanism, then new complications spring up.

For example, would a private hospital or doctor practicing in an office unrelated to an office have to get government clearance, a background check, or an official ID card in order to gain access to the NHIN or to a regional hub? What would be the criterion for access? What if someone had a criminal record? This discussion only hints at the enormity of just one limited aspect of the security issues any form of the NHIN will face.

And finally, on the issue of access control, it must be recognized that deterrence and prevention can conflict in practice. Some discussions of security in the NHIN emphasize

the need for accountability and thus the role of authentication. The National Research Council notes that "There is an inherent tension between authentication and privacy, because the act of authentication involves some disclosure and confirmation of personal information." [33] Medical identity theft will force some method of user authentication. If in fact patients are given choice, and some transactional record of the EHR as it passes through the NHIN, the attending physicians themselves may have to authenticate themselves, thus experiencing privacy issues as their data potentially becomes attached as a transactional access record to a patient EHR.

I do not say these things to discourage an NHIN. I am simply noting that the attendant security issues are extremely complex, and must be dealt with on a granular level before any form of the NHIN is architected. This will involve a great deal of effort from many sectors apart from and including healthcare.

C. *A Series of Regional Hubs vs. A Centralized National Network*

There has been a good bit of discussion about whether the NHIN should be conceived of as a single national system or one comprised of a set of regional hubs. Certainly the technology architectures change between the two models, for example, there would not be a single centralized database in a regional structure. However, core policy issues of patient choice, consent, and privacy do not fundamentally change.

For this reason, I think it is important to focus on the underlying policy issues regarding the NHIN prior to focusing on this question of regional versus national. However, having said that, if forced to give an answer, I favor a regional approach versus a centralized network for many technical and policy reasons. I believe the approach of creating a "floor" of standards upon which the states could creatively build and experiment should be the focus of any form of networked architecture.

III. Ten Proposed Questions to Ask Going Forward

In light of the challenges posed by the development, implementation, and successful adoption of EHRs and the NHIN, I have devised a set of ten questions I believe must be answered and set forth to the public prior to moving forward. I respect the questions the Committee set forth for this hearing. I also would like to note that the following questions are of central importance and answering them in a very public fashion should happen long before technical plans are undertaken.

- Will all patients be able to opt-out of an EHR system and/or an NHIN system if they so choose?

- Will only selected categories of individuals be able to opt-out of an EHR or NHIN system? If so, how will those categories of individuals be determined in a fair fashion, and how will individuals have the opportunity to appeal for opt-out if they are not included in a category of people allowed to opt-out?

- Will patients be able to access, correct, delete their own EHRs, as well as view transactional records of their EHR access, among other rights? In short, will patients be able to enjoy the full set of established Fair Information Principles in regards to the handling of their medical data?

- How will health care providers be able to guarantee patient identity in an EHR or NHIN system, with a specific view toward identity theft and fraud, while still protecting patient privacy?

- What breach prevention regulation is appropriate to undertake to encourage the protection of stored and in-transit EHRs and other medical data?

- Should one-time blanket consent be appropriate for all uses of EHR or NHIN data, or should there be a revocable consent that allows patients to choose who or what entities have access to their medical data, and for what purposes?

- What will the NHIN cost?

- Will the savings associated with the NHIN be enough to cover the cost? If no, how will that deficit be managed, and how will that impact patient care?

- How, specifically, will the NHIN be secured in all its aspects, and what entity or entities will bear that ongoing cost?

- If the consequences of the implementation of EHRs or the NHIN are less security and less privacy, then how will those implementing the system inform the public and Congress of this, and will this information come in advance of the implementation of the system?

IV. The Role of Fair Information Practices in a Digitized Medical Information Environment

Members of the committee will no doubt be familiar with the concept of Fair Information Practices from their work with HIPAA. It is my hope that the committee, as it seeks the answers to the questions I have posed, will use the most robust possible set of Fair Information Practices as a guide.[34] Fair information practices are not invariant, but most codes of fair information practices include these elements:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Compliance with all of these basic principles is especially important for a system which will contain and disseminate highly personal information of the utmost sensitivity.

V. Conclusion

There is an increasing amount of public discussion about EHRs and the NHIN. A number of political figures, vendors, doctors, and other interested parties generally state that EHRs will save lives and reduce costs.[35] Time magazine quoted an expert as saying that " ...the advent of electronic health records will be as significant as the discovery of penicillin." [36] It is true that a recent poll showed that Americans approve of EHRs, [37] but positive early polls and hyperbole are not enough to ensure ultimate public acceptance and success of either EHRs or an iteration of the NHIN. It is incumbent upon this Committee to ask the challenging questions and to find substantive, reasonable, and informed answers before anything is ventured or any data architectures are put in place.

We are living in a world which is transitioning from analog to digital. It is only logical that medical information should make the transition, too. I urge the Committee to consider that in a digital world with all of its varied implications, that patient choice is crucial to build into the policy and infrastructure. Providing patients with robust choice, privacy and confidentiality is an important part of the incentive individuals will need before entrusting their information to a new system.

In matters such as EHRs and the NHIN it is especially important that policy decisions precede technology decisions. I applaud the Committee members for making a good-faith effort to do just that by holding this meeting. I welcome any questions the Committee members may have.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum

Endnotes

[1] Executive Order 13335, Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator (Washington, D.C.: Apr. 27, 2004).

[2] See <http://www.worldprivacyforum.org/> . WPF and EFF comments on NHIN.

[3] World Privacy Forum report, 2003 Job Search Privacy Study, "Job Searching in the Networked Environment: Consumer Privacy Benchmarks. See < http://www.worldprivacyforum.org/workplace/wpfjobstudy.pdf>

[4] See < http://www.attorneygeneral.com/press/release.cfm?p=63807E79-F7D8-C5FB-113945CD4CCB12C7>.

[5] The Lufkin Daily News, 15 July 2005, Police Report.

[6] See "Medi-Cal Fraud Flourishing on Black Market,"
Jason Kandel, 7 August 2005, Los Angeles Daily News.

[7] "OPP Charge Man with Identity Theft," 5 August 2005, Canada NewsWire.

[8] GAO Report GAO-05-309R, Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology, 16 February, 2005. See <http://www.gao.gov/htext/d05309r.html>.

[9] Ibid.

[10] "Disaster-proofing your EHR," Lowes, Robert. 3 June 2005, Medical Economics.

[11] "Federal policies push information technology," 1 December 2004, Sherry Boschert, Skin & Allergy News.

[12] "Electronic Medical Records; Lumetra leads national project for adoption of electronic health records,"14 August 2004, Obesity, Fitness & Wellness Week.

[13] "Letters sent to 16,000 whose records taken from hospital," The Associated Press, April 26, 2005.

[14] "Patients' private data put online," San Jose Mercury News, 11 March 2005, Barbara Feder Ostrov.

[15] "Stolen computers expose personal data on 185,000 patients," The Associated Press, 8 April 2005, Rachel Konrad.

[16] "Privacy Breaches: Employees Removing Confidential Records," Report on Patient Privacy, March 2005.

[17] See http://www.dhs.ca.gov/mcs/Public%20Notices/default.htm>.

[18] "Duke: Computer hacker hits Duke med center sites,"U-Wire, 9 June 2005.

[19] HIPAA Wire at: < http://medicalnewswire.com/artman/publish/article_6140.shtml>.

[20] See http://www.summitdaily.com/article/20050802/NEWS/50802002>.

[21] "Medical firm's files with personal data stolen; Key information on 57,000 at risk," Arizona Republic, 13 July 2005, Matt Hanson.

[22] See HIPAA Advisory, http://www.hipaadvisory.com/news/recentnews.htm> Last visited August, 2005.

[23] See Gainesville Sun, <http://www.gainesville.com/apps/pbcs.dll/article?AID=/20050827/LOCAL/208270336/1078/news>.

[24] See generally National Academy of Sciences, For the Record: Protecting Health Information (1997) at 73 (Figure 3.1, flow chart of a hypothetical patient's health information).

[25] National Academy of Sciences, For the Record: Protecting Health Information at 54(1997).

[26] See "Costly Conversions: Switching to electronic medical records is an idea whose time has come. So why hasn't it?" Wall Street Journal, June 20, 2005, Kathryn Kranhold.

[27] "Nationwide Network Would Require $156B Initial Investment," 2 August 2005, American Health Line.

[28] HHS report: Decade of Health Information Technology at <http://www.hhs.gov/onchit/framework/hitframework.pdf>.

[29] "NHIN save lives reduce costs E-records vital to health strategy," 2 August 2004, Dibya Sarkar, Federal Computer Week. Also see "Rx For Better Health Care; Interoperable electronic health records promise to streamline health care delivery, improve quality and help contain costs. But financing, a lack of standards and the scope of implementation stand in the way," 31 January 2005, Kym Gilhooly, Computerworld.

[30] Computer Science and Telecommunications Board, National Research Council, IDs – Not That Easy: Questions About Nationwide Identity Systems at 42 (2002).

[31] Computer Science and Telecommunications Board, National Research Council, Who Goes There? Authentication Through the Lens of Privacy at 10, (2003).

[32] Ibid at 11.

[33] Ibid at 5-7, (finding that "[a]uthentication can affect decisional privacy, information privacy, communications privacy, and bodily integrity privacy interests"); id. at 178 ("In the case of government, respecting the legitimate function of anonymity is even more crucial."

[34] OECD, Guidelines on the Protections of Privacy and Transborder Flows of Personal Data, 1980. < http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html> .

[35] See for example "E-records vital to health strategy," 2 August 2004, Dibya Sarkar, Federal Computer Week.

[36] "The e-Health Revolution How a bipartisan bill from Hillary Clinton and Bill Frist could help jump-start a new kind of health-care reform," 27 June 2005, Bill Saporito, Time.

[37] "Americans Overwhelmingly Back Digital Health Records Concept," 21 July 2005, CMP TechWeb.