HEALTH PRIVACY PROJECT

January 18, 2005

David J. Brailer, M.D., Ph.D.
National Coordinator for Health Information Technology
Department of Health and Human Services
Attention: NHIN RFI Responses
Hubert H. Humphrey Building, Room 517D
200 Independence Avenue, S.W.
Washington, DC 20201

Re — NHIN RFI Responses

Dear Dr. Brailer,

The Health Privacy Project and the undersigned organizations are submitting these comments regarding the adoption of an interoperable electronic health records system in response to the Request for Information (RFI) published in the Federal Register on November 15, 2004. The Health Privacy Project (HPP) is a 501(c)(3) nonprofit organization dedicated to raising awareness about the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and community level. The Health Privacy Project conducts research and analysis on a wide range of health privacy issues, including objective analysis of the HIPAA Privacy Rule and state health privacy laws, genetics and workplace privacy, e-health activities, and bioterrorism and public health surveillance initiatives. HPP also coordinates the Consumer Coalition for Health Privacy (CCHP), which is comprised of over 100 major organizations representing a broad range of both consumers and health care providers. A complete list of Coalition participants, as well as all of the Project's resources related to health privacy, can be found at our web site, www.healthprivacy.org.

The Health Privacy Project has long been actively engaged in the ongoing discussion about the adoption of an interoperable system of electronic health records that are available at the point of care. In this capacity, HPP has produced several publications focused on the importance of building on the principle of privacy as new health information technologies are conceived, including *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*, *Virtually Exposed: Privacy and E-Health*, and *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users*. HPP also continues to serve on the Privacy and Security Working Group of Connecting for Health, a public-private collaborative established by the Markle Foundation focused on addressing barriers to the development of an interoperable health information infrastructure.

The Health Privacy Project's mission is to foster greater public trust and confidence in the health care system, thereby enabling people to more fully participate in their own care and in research without putting themselves at risk for unwanted—and unwarranted—intrusions. It is wrong to force people to choose between seeking health care and safeguarding their privacy. And, unfortunately, when people do have to choose, they very often choose to forgo quality health care. As captured by

a 1999 California HealthCare Foundation survey, one out of every six Americans withdraws from full participation in their own health care out of fear that their medical information will be used without their knowledge or permission. These privacy-protective behaviors include patients providing inaccurate or incomplete information to doctors, patients paying out of pocket to avoid a claim being submitted, and people avoiding care altogether.

These comments are intended to provide an examination of the movement towards a National Health Information Network (NHIN) through the scope of patient privacy. The national conversation about the development of electronic connectivity has largely overlooked the fundamental need to build in privacy and security protections at the outset. The foundation of any successful health information network is the trust and cooperation of consumers, and the development of a NHIN must start first with a serious effort to engage, empower, and leverage the positive cooperation of patients.

General 1-7

The Health Privacy Project and the undersigned organizations fully support and encourage the development of an interoperable national health information network that is built on the concepts of patient control, privacy, and participation.

In this era of health care fragmentation, most people see many different providers, in many different locations, throughout their lives. To get a full picture of each patient, a provider must request medical records from other providers or the patient, a burdensome process that rarely produces a thorough and accurate patient history, and sometimes produces disastrous errors. According to the Institute of Medicine, more than 500,000 people annually are injured due to avoidable adverse drug events in the United States. Linking medical records is, literally, a matter of life and death.

The technology exists to create linked health information networks that deliver pertinent information at the point of care. A successful NHIN would drastically improve quality of health services, offering the potential for the quick exchange among authorized users of more accurate and coherent personal health information. Implemented correctly, NHIN could also incorporate stronger privacy protections, improving patient access to and control over their own health information. By offering more consumer-friendly methods of access and control, NHIN could also empower patients and significantly enhance their participation in their own care, with untold benefits to both individuals and the general public.

But the benefits of electronic access to health information are matched by significant risks, and the primary concern for providers and patients alike is privacy. In order to develop a system that enhances quality of care, privacy and security must be addressed from the outset. If a national system of electronic connectivity is to be successful, it must be built on the principles of patient participation and control, and it must reflect the critical role privacy plays in the health care system. There is no faster way to jeopardize the success of a national health information network than to forgo a comprehensive and thoughtful application of protecting individually-identifiable health information. And there is no better way to win the public's trust, confidence, and informed participation than to offer proactive, concrete assurances that personal health information will be protected.

The Health Privacy Project and the undersigned organizations view a successful NHIN as a system of electronic health information built on connecting local and regional systems.

A successful NHIN would harness the ability to connect localized health information networks throughout the country, with networks participating through the ability to "talk" to one another (i.e. requesting health information through secure means). A successful NHIN would be a de-centralized "network of networks" that functions on the ability of authorized doctors, hospitals, labs, etc. to request personal health information. Upon approval, a NHIN system would provide the mechanism through which health information could be exchanged over a secure system. This setup ensures that control over personal health information stays where it belongs—with the patient and in consultation with their doctor.

To ensure patient privacy, personal health information would be shared on request and only with authorized users. A successful NHIN should be able to exchange data without the use of any type of national ID, and it must be able to incorporate the principle of "minimum necessary," whereby only the minimum pertinent health information is shared. Further, a NHIN should be consistently tested to ensure data security.

A NHIN must be built on a set of technical and policy requirements that users must adopt. This policy framework should establish enforceable guidelines that are required for inclusion and based on the principles of privacy and security. This type of membership requirement will play an important role in establishing clear and strong policies and standards that ensure a commitment to establishing trust.

The Health Privacy Project and the undersigned organizations strongly urge the development of a strong public education and participation effort.

The most glaring fracture in the ongoing discussion about building a NHIN is the lack of consumer awareness and participation. Patients have the largest stake in the development of a national health information network, and yet, they have been severely underrepresented in the national conversation about linking health information. Their absence is only reflective of the marginalized role patients currently play in the health care arena, but it presents an enormous barrier to achieving an effective national health information network.

Already, the public is anxious about how their privacy is protected in the health care arena. A California HealthCare Foundation survey found that one in five persons believe that their offline personal health information has been used inappropriately, without their knowledge or consent.[1] And a January 2000 survey showed that 75 percent of internet users are concerned about health websites sharing information without their permission.[2]

At the same time, Americans are open to developments in health information technology. According to a 2002 Harris poll, approximately 90 percent of American adults with internet access

[1] California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (Oakland: CHCF, January 1999).
[2] Cyber Dialogue, *Ethics of Survey of Consumer Attitudes about Health Web Sites* (Oakland: CHCF, January 2000).

would like to communicate with their doctors by e-mail.[3] Additionally, many Americans (37 percent) would be willing to pay out-of-pocket to communicate with their doctors online.[4] In a 2003 Connecting for Health survey, over 60 percent of Americans said they wanted to receive the specific services (such as tracking test results, amending records, and transferring health information) that a more electronically connected health care infrastructure could provide.[5]

It is imperative that both public and private entities reach out to consumers with consistent messages about the benefits of electronic connectivity and the importance of accessing their own health information. As a part of this effort, it is critical that consumer advocates are included in strategic discussions about the development of a NHIN. As the process moves forward, it will be increasingly important to foster a more open deliberation that allows for honest evaluations about the impact on patient privacy.

In general, Americans appear to support a movement towards developments in health information technology. Still, there is a very real need to reach out, energize, and harness the momentum only a consumer-based drive to the creation of a NHIN could provide. Consumers need to be informed, assertive, and active in their own care if a NHIN is to meet its full potential. Educating the public is central to creating a system that respects the privacy and security boundaries patients feel comfortable with, and, thus, realizing the need for adequate patient participation.

A NHIN must be rooted in fundamental principles of privacy.

The NHIN structure must build on established principles of patient privacy and control. Trust is at the nucleus of the doctor-patient relationship, and the development of a NHIN must establish controls that enforce privacy protections and consistently reflect the imperative that patients have confidence that their sensitive health information is secure.

A NHIN must, at a minimum, adopt the protections afforded consumers under the HIPAA Privacy Rule and be flexible to incorporate more stringent state privacy laws.

In many ways, the HIPAA Privacy and Security Rules paved the way for electronic health care initiatives to move forward. The Rules recognize that along with the benefits of easier access to health information, the move to electronic communications also presents privacy risks, and the Rules address the importance of ensuring privacy in all electronic transactions.

Based on the principle of informed consent, the Privacy Rule acknowledges that in order to have meaningful control over personal health care decisions, patients must have meaningful access to and control over their own personal health information. The most basic tenet of the HIPAA Privacy Rule is that personal health information should be kept and shared only where it belongs—in the health care arena. The Privacy Rule grants Americans many important rights, including access to

---

[3] Harris Interactive, "Patient/Physician Online Communication: Many Patients Want It, Would Pay for It, and It Would Influence their Choice of Doctors and Health Plans." April 10, 2002. Online. Available. http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2002Vol2_Iss08.pdf

[4] Harris Interactive, "Patient/Physician Online Communication: Many Patients Want It, Would Pay for It, and It Would Influence their Choice of Doctors and Health Plans." April 10, 2002. Online. Available. http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2002Vol2_Iss08.pdf

[5] Connecting for Health, *Achieving Electronic Connectivity in HealthCare: A Preliminary Roadmap from the Nation's Public and Private Sector Healthcare Leaders* (Markle Foundation: July 2004).

their own medical records and notice of how their doctors and health plans may use their information. The law also assures Americans that law enforcement officials cannot access their medical records without proper legal process, and that health care providers and plans are prohibited from sharing information with employers. Furthermore, the law gives the Department of Health and Human Services and the Department of Justice the authority to impose civil and criminal penalties for violations and leaves states free to enact more stringent privacy protections.

Covered entities will be required to comply with the Security Rule on April 21, 2005, except for small health plans, who will have an additional year to prepare. The Security Rule instructs covered entities to "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[6] The rule specifically instructs covered entities to implement security measures "to ensure that electronically protected health information is not improperly modified without detection until disposed of" and to implement "a mechanism to encrypt electronic protected health information whenever deemed appropriate."[7] Because these implementation specifications are "addressable," if a covered entity deems them inappropriate it may implement alternative measures. Covered entities may choose not to adopt addressable specifications as long as they document why the specifications are not reasonable and appropriate, and implement equivalent alternative measures, if reasonable and appropriate.[8]

Both the HIPAA Privacy and Security Rules provide an important floor of protection for patients' personal health information, but the Rules are just that—a *floor* of protection. In many ways, neither of these Rules adequately addresses the concept of a NHIN structure. With this in mind, a NHIN should start with the applicable safeguards afforded under the HIPAA Privacy and Security Rules as a foundation for more meaningful protections.

Participation in a NHIN must be voluntary and based on the principle of informed consent.

Before agreeing to participate, patients should be adequately informed and fully understand how their personal health information will be collected, stored, and used within a NHIN. This information sharing process should include a full disclosure of all elements central to network functioning and must be presented in a consumer-friendly manner. Patients should also be acutely aware of all established policies and procedures that relate to the security (including who is authorized to access their information) of a network.

A patient's decision to participate in a NHIN must be voluntary. Once being comprehensively informed, patients should have the unqualified right to choose whether they will participate or not—in whole or in part. Further, patients should have the ability to opt-in or out of the system at any time, without coercion or pressure.

Patients must have significant control over their own personal health information.

---

[6] 45 C.F.R. § 164.312(e)(1)
[7] 45 C.F.R. § 164.312(e)(2)(i-ii)
[8] 45 C.F.R. § 164.306(d)(3). In determining whether a specification is reasonable and appropriate, a covered entity may consider factors such as "the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation" (68 F.R. 8336)

Patients should have significant control over the flow of data as it relates to their personal health information. In consultation with their providers, patients should be able to decide what information is included in the NHIN, and they must have the ability to designate who will have authority to manage their personal health information. Patients should have the right to exercise this authority in whole or in part with regard to particular pieces of personal health information.

A NHIN structure must allow consumers to access their personal health information in an affordable and timely manner.

The right to access information held about oneself is essential to privacy. Health care providers keep detailed records on the medical histories, diagnoses and treatments of each of their patients. But until recently, patients had no federal right to see and copy their own medical records. The HIPAA Privacy Rule changed that, and it is crucial that a NHIN recognize this powerful tool in promoting patient's participation and improving quality of care.

Access to personal health information is essential to strong privacy protections and quality health care. In the health care arena, access to one's own medical records has been shown to encourage participation in care and compliance with treatment. A 2003 review of studies on patient access to medical records found that access provides benefits such as enhanced doctor-patient communication.[9] Americans support a shift to electronic modes of communication and access when it comes to the delivery of health care. In a 2003 survey, over 70 percent of Americans reported that they believed accessing their own personal health records online would improve the quality of their health care.[10]

A NHIN must incorporate the right to access medical information. In doing so, patients should be able access their entire available record (all information available to other authorized users) in both an electronic and paper-based capacity and without burdensome fees. A NHIN must provide a practical method for authenticating individual patient users, without the need for provider consultation. Further, the NHIN structure must ensure that the information is shared in a method that patients can comprehend. In addition to considerations about translating medical codes and terminology, there should be an earnest discussion about the ability to overcome language barriers in a NHIN system. Patients with disabilities should be assured the right to access their medical information in accessible formats and via accessible technology. Patients should also have the right to access information about disclosures providers made about their personal health information, and they should be able to easily transfer all or portions of their personal health information from one provider to another.

A NHIN system must afford consumers the opportunity to contribute to their medical record and amend/supplement their health information at any time.

Patients should have the ability to contribute information to their medical record, as long as it is clear which information is contributed by the patient. Patients must also be able to request an

[9] Stephen E. Ross, MD and Chen-Tan Lin, MD, "The Effects of Promoting Patient Access to Medical Records: A Review," J Am Med Inform Assoc. 2003 March; 10(2): 129-138.
[10] Markle Foundation. Connecting for Health. "Americans Want Benefits of Personal Health Records." June, 5 2003. Online. Available. http://www.connectingforhealth.org/resources/phwg_survey_6.5.03.pdf

amendment or supplement to their personal health information, and they should receive a timely response to their request.

Strong enforcement regulations should be in place to ensure adherence to privacy and security policies.

There should be constructive enforcement regulations in place that support privacy and security policies and procedures. Patients should have recourse if their medical privacy is violated. Strong enforcement regulations will send a powerful message to patients and providers alike that privacy and security protections are important. It is simply not enough for participating entities to self regulate. Enforcement provisions should carry the force of law, and entities must be monitored and held accountable for violations of privacy and security policies. Again, in order to ensure that patients will accept and participate in a NHIN, they must be assured that the privacy of their sensitive medical information comes first.

Conclusion

Health information technology is a promising antidote to many problems that currently plague our health care system. There is no underestimating the vital importance of the ability to efficiently access health information at any point of care, emergency or otherwise. However, with the promise of electronic connectivity comes concerns about patient privacy and cooperation. The biggest barrier to the development of an efficient NHIN system is the one that we construct by ignoring the importance of building a national network on the principles of privacy, control, and security. The only way to move towards our collective goal of improving our nation's health care infrastructure with the technological tools we already carry is to first and foremost address the privacy concerns of patients.

If you have any questions about these recommendations, please contact Emily Stewart, HPP's Policy Analyst at: 202-721-5614 or estewart@healthprivacy.org.

Thank you for your consideration,

Sincerely,

Health Privacy Project
AFL-CIO
National Association of People with AIDS (NAPWA)
American Mental Health Counselors Association
American Association of People with Disabilities