Testimony of

Janlori Goldman, Director
Health Privacy Project

Before the
Senate Special Committee on Aging

Regarding Implementation of the HIPAA Privacy Regulation

September 23, 2003

To Committee Chairman Craig, Senator Breaux, and Members of the Committee:

On behalf of the Health Privacy Project, I am very appreciative for the opportunity to testify before you today on the medical privacy regulation mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The landmark privacy rule is the first comprehensive federal law aimed at safeguarding the confidentiality of patient records within the health care system. In mandating the law, Congress recognized that protecting patient privacy is central to fostering both access to health care and high quality health services. Since the April 14, 2003 date by which health care providers, plans, and others were required to comply with the law – following more than two years for implementation – there has been both confusion and misunderstanding about certain provisions of the law. Some of the confusion was anticipated, and could have been addressed through more rigorous guidance and education from regulators and professional associations. Nevertheless, many of the initial glitches have been resolved and clarified, and phone calls regarding implementation questions to both the HHS Office of Civil Rights (OCR) and the Health Privacy Project have decreased in the last couple of months. In addition, OCR's guidance over the past few months has grown increasingly comprehensive and targeted to the bulk of questions and concerns that have arisen.

However, where misinterpretation persists, we urge that both the HHS Office of Civil Rights, and the professional and trade associations representing providers, plans, and others affected by the law, aggressively step up their technical assistance and guidance. We believe that resources should be devoted to proper and vigorous implementation, and not to using misunderstanding and mishap to build public opposition to the law. Evidence of confusion must commit us to better educating the public, not to undermining support for the medical privacy protections the public clamored for decades. To better educate consumers in a simple, easy-to-read format, the Health Privacy Project published "Know Your Rights," which is available as a brochure and on our web site.

Halfway through the two year compliance period, a California HealthCare Foundation survey of health care organizations indicated that although implementation efforts were well underway, there were areas of confusion and misinterpretation. The health care industry and regulators were put on notice at that time that more resources were needed to ensure the law was better understood. To better educate consumers in a simple, easy-to-read format, the

Health Privacy Project published "Know Your Rights," which is available as a brochure and on our web site. At this stage, we urge Congress to request that a follow-up study be conducted, possibly by GAO or the NCVHS, that measures the status and impact of implementation.

Our testimony highlights the major myths about the privacy rule, and sets the record straight with the facts. Our testimony also addresses the cost of implementing the privacy rule, citing this administration's own findings that privacy costs will be significantly offset by savings achieved through standardizing transactions and code sets. Savings will also be achieved as people more fully participate in their own care, thereby reducing the risk of undiagnosed and untreated conditions. We also include here a brief overview of the history of HIPAA, and the urgent public need for a medical privacy law.

The Health Privacy Project

The Health Privacy Project is dedicated to broadening access to health care, and improving the quality of care by ensuring that people's medical information is safeguarded in the health care arena. The Project conducts research and analysis on a wide range of health privacy issues, including objective analysis of the new regulation, a compilation of state health privacy laws, genetics and workplace privacy, reports on e-health and health web sites, and an initiative on public health emergencies. In addition, the Health Privacy Project coordinates the Consumer Coalition for Health Privacy, comprised of over 100 major groups representing consumers, health care providers, and labor, disability rights, and disease groups. Coalition participants include AARP, the American Nurses Association, Bazelon Center for Mental Health Law, National Multiple Sclerosis Society, National Association of People with AIDS, National Organization for Rare Disorders (NORD), and the Genetic Alliance. 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.

Urgent Need for Health Privacy

Previously, the lack of a national health privacy law had a negative impact on health care, both on an individual as well as at the community level. A 1999 survey by the California HealthCare Foundation documented that one out of every six people withdraws from full participation in their own care out of fear that their medical information will be used without their knowledge or permission. These privacy-protective behaviors include patients providing false or incomplete information to doctors, doctors inaccurately coding files or

leaving certain things out of a patient's record, people paying out of pocket to avoid a claim being submitted, or in the worst cases, people avoiding care altogether.

More specifically, a 1997 survey documenting people's fears about genetic discrimination showed that 63 percent of people would not take genetic tests if health insurers or employers could obtain the results. (*Genetic Information and the Workplace,* issued on January 20, 1998 by the U.S. Departments of Labor, Health and Human Services, and Justice, and the U.S. Equal Employment Opportunity Commission). And, a study involving genetic counselors documents that fear of discrimination is a significant factor affecting willingness to undergo testing and to seek reimbursement from health insurers. (Hall, Mark A. and Stephen S. Rich, *Genetic Privacy Laws and Patients' Fear of Discrimination by Health Insurers: The View from Genetic Counselors*, 28 Journal of Law, Medicine & Ethics 245-57 (2000).)

An April 2001 Harris survey documents that nearly four out of ten (40%) people with multiple sclerosis said they have lied or failed to disclose their diagnosis to colleagues, co-workers, friends or even family members out of fear of job loss and stigma.

These survey figures come to life in the daily media reports of people being harmed by the inappropriate use of their health information. To highlight just a few:

- Just recently, the alleged victim in the Kobe Bryant rape case had her medical records regarding a previous hospitalization released by hospital staff, who it appears violated the HIPAA privacy regulation. The hospital's own motion following the unauthorized disclosure argues that the records were shared in violation of the rule, and requests that they be returned to the hospital or destroyed.

- The medical records of an Illinois woman were posted on the Internet without her knowledge or consent a few days after she was treated at St. Elizabeth's Medical Center following complications from an abortion at the Hope Clinic for Women. The woman has sued the hospital, alleging St. Elizabeth's released her medical records without her authorization to anti-abortion activists, who then posted the records online along with a photograph they had taken of her being transferred from the clinic to the hospital.

- Terri Seargent was fired from her job in North Carolina after being diagnosed with a genetic disorder that required expensive treatment. Three weeks before being fired, Terri was given a positive review and a raise. As such, she suspected that her employer, who is self-insured, found out about her condition, and fired her to avoid paying costly medical expenses.

- Several thousand patient records at the University of Michigan Medical Center inadvertently lingered on public Internet sites for two months. The problem was discovered when a student searching for information about a doctor was linked to files containing private patient records with numbers, job status, treatment for medical conditions and other data.

- Joan Kelly, an employee of Motorola, was automatically enrolled in a "depression program" by her employer after a prescription drugs management company reported that she was taking anti-depressants.

- The Florida Attorney General's office investigated the marketing practices of Eckerd Drug Company to determine whether or not the company violated customers' privacy. When customers picked up their prescriptions, the chain drug compnay had them sign a form not only acknowledging receipt of a prescription but also authorizing the store to release their prescription information for future marketing purposes. The form apparently did not adequately inform customers that they were authorizing the commercial use of their medical information. According to the Attorney General's investigation, no customer or store employee interviewed was aware of the fact that the customer had actually signed an authorization for marketing purposes. As part of a settlement, Eckerd agreed to change its policies to better protect patient privacy, including restricting the direct marketing of prescription drugs to customers who have given written consent to use their medical information for such purposes. The company also agreed to fund a $1 million ethics chair at the Florida A & M School of Pharmacy.

- Eli Lilly and Co. inadvertently revealed 600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac. In the past, the e-mail messages were addressed to individuals. The message announcing the end of the reminder service, however, was addressed to all of the participants.

- Last year, a hacker downloaded medical records, health information, and social security numbers on more than 5,000 patients at the University of Washington Medical Center. The University conceded that its privacy and security safeguards were not adequate.

In the absence of a federal health privacy law, these people suffered job loss, loss of dignity, discrimination, and stigma. Had they acted on their fears and withdrawn from full participation in their own care – as many people do to protect their privacy – they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have been forced to choose between shielding themselves from discrimination, or receiving health care services.

The Genesis of the Privacy Rule

The HIPAA Privacy Rule is a major victory for all health care consumers, and takes a significant step toward restoring public trust and confidence in our nation's health care system. The regulation fills the most troubling gap in federal privacy law, setting in place an essential framework and baseline on which to build. Each one of us stands to benefit from the Privacy Rule in critical ways, including greater participation in the health care system, improved diagnosis and treatment, more reliable data for research and outcomes analysis, and greater uniformity and certainty for health care institutions as they develop privacy safeguards and modernize their information systems.

Most notably, the Privacy Rule: requires health care providers to give people notice of the rights under the new law and to inform people about how their health information will be used; grants people the right to see and copy their own medical records; imposes limits on disclosing patient records to employers; broadens the scope of protection for people whose health information is used by privately-funded researchers; puts safeguards in place for disclosure to law enforcement; and allows for civil and criminal penalties to be imposed if the Rule is violated.

The Privacy Rule was issued by the Department in December 2000 in response to a mandate from Congress included in the 1996 Health Insurance Portability and Accountability Act (HIPAA), which required that if Congress did not enact a medical privacy statute by August 1999, then HHS was required to promulgate regulations. Congress did miss the deadline, and after the mandate shifted to HHS, the rule was the subject of a lengthy, thorough, and robust rule-making process – both before and since it was released in December 2000.

Despite intense pressure from some in the health care industry, the Bush Administration allowed this important regulation to go into effect in April 2001. The first implementation guidance issued by the Department on July 6, 2001, addressed the many misstatements and exaggerations that some in the industry had spread about the Privacy Rule. That guidance—and much of the guidance that followed-- appears aimed at calming industry fears, promoting clarity, and fostering compliance with the regulation.

When President Bush allowed the Privacy Rule to go into effect in April, 2001 he issued a strong statement about the need to protect patient privacy and foster confidence that people's "personal medical records will remain private." The President also pledged during his campaign to support a law requiring that a "company cannot use my information without my permission to do so," and expressed support for strong laws protecting medical and genetic privacy. In fact, William Safire dubbed him the "privacy President" in a New York Times column shortly after the Privacy Rule went into effect.

We believe that the Privacy Rule – as finalized – could go farther in protecting patients. One shortcoming is that the rule only directly regulates providers, plans and clearinghouses, and does not directly regulate employers, pharmaceutical companies, workers compensation insurers, and many researchers. Also, the regulation lacks a private right of action that would give people the right to sue if their privacy is violated. Under HIPAA, only Congress and the states are empowered to address these limits. Other weaknesses, such as allowing sensitive medical information to be used for marketing without patient knowledge or consent, are within the HHS' authority to regulate.

The history of the privacy rule's genesis is important here. Many in the health care industry pressed Congress to include in HIPAA the mandate for transaction and code set regulations to be developed (known pithily as "Administrative Simplification"). The industry's mission at that time was to put in place a common language for the coding of certain patient encounter data so as to streamline billing, and create greater efficiency and uniformity in the processing and use of certain health data. Substantial cost savings was the major driver for including the language in HIPAA. At the same time, Congress acknowledged that a streamlined electronic health information network posed heightened risks to patient privacy, as collecting and sharing health information moved out of a filing cabinet available to a few and into a linked online network available to many. Congress intended the privacy law timeline – which is a part of the administrative simplification section of HIPAA—to coincide

with the implementation of the uniform transaction and code sets, as well as the security rules. Both Congress and the Executive Branch recognized that a key to the success of a national health information infrastructure was to build privacy and security rules in at the outset. In fact, a report released in June 2003 by the Connecting for Health public/private collaborative of the Markle Foundation reached the same conclusion.

Myths and Facts

Both the 1996 Congress and the two recent administrations agree that a privacy law is needed to ensure that sensitive personal health information can be shared for core health activities, with safeguards in place to limit the inappropriate use and sharing of patient data. The HIPAA privacy rule takes critical steps in that direction to require that privacy and security be built in to the policies and practices of health care providers, plans, and others involved in health care. Despite the law's clear purpose and scope, a lack of widespread and consistent public education, training, and technical assistance over the past 2 and one half years, has given rise to a number of persistent and destructive myths.

The following are some common myths regarding the Rule and the facts about what the law actually says.

Myth #1: One doctor's office cannot send medical records of a patient to another doctor's office without that patient's consent.

FACT: No consent is necessary for one doctor's office to transfer a patient's medical records to another doctor's office for treatment purposes. The Privacy Regulation specifically states that a covered entity "is permitted to use or disclose protected health information" for "treatment, payment, or health care operations," without patient consent. As HHS explains, "treatment" includes "consultation between health care providers regarding a patient and referral of a patient by one provider to another." HHS states that providing health records to another health care provider for treatment purposes "can be done by fax or other means." §§164.502(a)(1)(ii), 164.506(a), http://www.hhs.gov/ocr/privacysummary.pdf (page 5), http://www.hhs.gov/ocr/hipaa/ (FAQ section, page 1, questions 6 & 12).

Myth #2: The HIPAA Privacy Regulation prohibits or discourages doctor/patient emails.

FACT: The Privacy Regulation allows providers to use alternative means of communication, such as email, with appropriate safeguards. Doctors and other healthcare providers may continue to communicate with patients via email. Both the HIPAA Privacy and Security Regulations require providers to use reasonable and appropriate safeguards to "ensure the confidentiality, integrity, and availability" of any health information transmitted electronically, and to "protect against any reasonably anticipated threats" to the security of such information. Therefore, a covered entity is free to continue using email to communicate with patients, but should be sure that adequate safeguards, such as encryption, are used. §§ 164.522(b)(1)(i), 164.306(a)(1)-(2), (d)(3)(i)-(ii), 164.312(e)(2)(ii).

Myth #3: A patient cannot be listed in a hospital's directory without the patient's consent and the hospital is prohibited from sharing a patient's directory information with the public.

FACT: The Privacy Rule permits hospitals to continue the practice of providing directory information to the public unless the patient has specifically chosen to opt out. The Regulation states that a health care provider, such as a hospital, may maintain a directory that includes the patient's name, location in the facility, and condition in general terms, and disclose such information to people who ask for the patient by name. The patient must be informed in advance of the use and disclosure and have the opportunity to opt out of having his or her information included in the directory. Emergency situations are specifically provided for in the Regulation, so if the patient is comatose, or otherwise unable to opt out due to an emergency, the hospital is permitted to disclose directory information if the disclosure is consistent with the patient's past known expressed preference and the provider determines disclosure is in the individual's best interest. The provider must provide the patient with an opportunity to object, "when it becomes practicable to do so." Any more restricted uses of directory information, such as requiring patients to ask to be listed in, or opt into, the directory, are either the hospital's own policy or confusion about the Privacy Regulation.
§164.510(a), http://www.hhs.gov/ocr/privacysummary.pdf (page 6), http://www.hhs.gov/ocr/hipaa/ (FAQ section, page 2, question 37).

Myth #4: Members of the clergy can no longer find out whether members of their congregation or their religious affiliation are hospitalized unless they know the person by name.

FACT: The Regulation specifically provides that hospitals may continue the practice of disclosing directory information "to members of the clergy," unless the patient has objected to such disclosure. Any requirement that the patient must list a specific church or any limitation on the practice of directly notifying clergy of admitted patients is either an internal hospital policy or based on a confused reading of the law.
§ 164.510(a)(ii)(A) http://www.hhs.gov/ocr/privacysummary.pdf (page 6).

Myth #5: A hospital is prohibited from sharing information with the patient's family without the patient's express consent.

FACT: Under the Privacy Rule, a health care provider may "disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual," the medical information directly relevant to such person's involvement with the patient's care or payment related to the patient's care. Uses and disclosures "for involvement in the individual's care and notification purposes" are clearly permitted. The Rule states that if the patient is present, the health care provider may disclose medical information to such people if the patient does not object. If the patient is unable to agree or object to disclosure because of incapacity or an emergency circumstance, the covered entity may determine whether the disclosure is in the best interests of the patient. The professional judgment of the health care provider should inform any decision regarding disclosure of protected health information to a family member or friend who is involved in the patient's care, as these disclosures are permitted, but not mandatory. If a hospital or other health care provider refuses to provide any relevant medical information to family members, it is again, the hospital policy, and not required by the Regulation.
§ 164.510(b)

Myth #6: A patient's family member can no longer pick up prescriptions for the patient.

FACT: Under the Regulation, a family member or other individual may act on the patient's behalf "to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information." The Regulation permits the health care provider to reasonably infer that doing so is in the patient's best interest and in accordance with professional judgment and common practice. HHS specifically explains that the Rule "allows a

pharmacist to dispense filled prescriptions to a person acting on behalf of the patient." Similarly, HHS issued guidance and a press release on July 6, 2001 that explicitly stated that "the rule allows a friend or relative to pick up a patient's prescription at the pharmacy." Therefore if pharmacies prohibit this common practice, it is their own policy, not one mandated by the HIPAA Privacy Regulation.
§ 164.510(b)(3), http://www.hhs.gov/ocr/privacysummary.pdf (page 6).

Myth #7: The Privacy Regulation mandates all sorts of new disclosures of patient information.

FACT: As HHS states, disclosure is mandated in only two situations: to the individual patient upon request, or to the Secretary of the Department of Health and Human Services for use in oversight investigations. Disclosure is permitted, not mandated, for other uses under certain limits and standards, such as to carry out treatment, payment, or health care operations, or under other applicable laws. Disclosure of protected health information has always been permitted for purposes such as national security, public health monitoring, and law enforcement, as well as many others. The Privacy Rule requires that patients be informed, through the notice of privacy practices, of these uses and disclosures. Nearly all of these uses and disclosures are permissive, so health care plans and providers may choose not to use or disclose medical information. §§ 164.502, 164.508, 164.512, 164.520, http://www.hhs.gov/ocr/privacysummary.pdf (pages 4-11).

Myth #8: The HIPAA Privacy Regulation imposes so many administrative requirements on covered entities that the costs of implementation are prohibitive.

FACT: The White House issued a report in March 2002 estimating the costs of implementing privacy over ten years at approximately $17 billion and estimating the savings incurred from putting the transaction standards in place over ten years at approximately $29 billion, thus saving the health care industry $12 billion overall. Further, there will be additional savings in the long term because patients will have more faith in the health care system, so they will be less likely to withhold vital information from their doctors, and will more readily seek care.

Myth # 9: Patients will sue health care providers for not complying with the HIPAA Privacy Regulation.

FACT: The HIPAA Privacy Regulation does not give people the right to sue. Even if a person is the victim of an egregious violation of the HIPAA Privacy Regulation, the law does not give people the right to sue. Instead, the person must file a written complaint with the Secretary of Health and Human Services via the Office for Civil Rights. It is then within the Secretary's discretion to investigate the complaint. HHS may impose civil penalties ranging from $100 to $25,000, and criminal sanctions ranging from $50,000 to $250,000, with corresponding prison terms, may be enforced by the Department of Justice. However, according to the interim final rule addressing penalties, HHS "intends to seek and promote voluntary compliance" and "will seek to resolve matters by informal means whenever possible." Therefore enforcement "will be primarily complaint driven," and civil penalties will only be imposed if the violation was willful. Such penalties will not be imposed if the failure to comply was due to reasonable cause and is corrected within 30 days from when the covered entity knew or should have known of the failure to comply. The standard is even higher for imposing criminal penalties. §§ 160.306, 160.312 (a)(1), 160.304(b), 42 U.S.C § 1320 et seq., http://www.hhs.gov./news/facts/privacy.html.

Myth #10: Patients' medical records can no longer be used for marketing.

FACT: Use or disclosure of medical information is explicitly permitted for certain health related marketing under the HIPAA Privacy Regulation. For example, communication about a plan's health related products or alternative treatments and services is not considered marketing for the purposes of the Rule—even if the health care provider is paid to encourage the patient to use the product or service. The 2000 version of the Privacy Rule required that patients be notified if the health care provider was paid to communicate about a health related product, be given the opportunity to opt out of future communications, and be informed of the identity of the source of the communication. The Bush Administration eliminated these safeguards from the Regulation. §§164.508(a)(3), 164.50, http://www.hhs.gov/news/press/2002pres/20020809.html.

Myth #11: If a patient refuses to sign an acknowledgment stating that she received the health care provider's notice of privacy practices, the health care provider can, or must, refuse to provide services.

FACT: The HIPAA Privacy Rule grants the patient a 'right to notice' of privacy practices for protected health information, and requires that providers make a "good faith effort" to get patients to acknowledge they have received the notice. The law does not grant health care providers the right to refuse to treat people who do not sign the acknowledgement, nor does it subject the provider to liability if a good faith effort was made. A health care provider or health plan "must provide a notice that is written in plain language" that informs the patient of "the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information." The HIPAA Privacy Rule requires a covered health care provider with direct treatment relationships with individuals to give the notice to every individual no later than the date of first service delivery to the individual, to provide a copy of the notice to the patient upon request, to post a copy of the notice in a prominent location, and to "make a good faith effort to obtain a written acknowledgment of receipt of the notice" except in emergency situations. The acknowledgment of the receipt of notice of the privacy practices is not a consent for treatment. It is not an authorization for the release of medical records. A patient's signature acknowledging receipt of the notice, or her refusal, does not create or eliminate any rights, so it should not be the basis for providing or refusing treatment.
§ 164.520(b)(1), (a)(1), (c)(2)(i)-(iii)

Myth #12: The HIPAA Privacy Rule imposes many new restrictions on hospitals' fundraising efforts so that fundraising becomes almost impossible.

Fact: According to the Rule, a hospital may use, or disclose to its "business associate" or an institutionally related foundation, demographic information and the dates of health care provided to an individual "for the purpose of raising funds for its own benefit, without an authorization [from the patient]." Such use or disclosure is not permitted unless disclosed in the notice of privacy practices. Any fundraising materials that the covered entity sends to an individual must include a description of how the individual may opt out of future fundraising communications. Therefore, the Rule does not hinder fundraising in the first instance, and if a covered entity wants to target specific patients it must include

this information in its notice of privacy practices. Hospitals must also make reasonable efforts to ensure that those who decide to opt out of receiving future fundraising communications do not continue to receive such communications. §§ 164.514(f)(1)-(2), 164.520(b)(1)(iii)(B).

Myth #13: The press can no longer access vital public information from hospitals about accident or crime victims.

Fact: HIPAA allows hospitals to continue to make public (including to the press) certain patient directory information - including the patient's location in the facility and condition in general terms - unless the patient has specifically opted out of having such information publicly available. Thus, if a patient has not opted out of being listed in a hospital directory, and a reporter knows the name of an accident or crime victim, the reporter can request directory information from a hospital, including the condition of the patient. HIPAA does prohibit the hospital from releasing anything more than directory information, without the patient's authorization. This HIPAA provision, however, is not a change from most existing state laws, which protect the confidentiality of patient information to varying degrees. Further, the HIPAA Privacy Rule does not directly cover the media, so once a reporter obtains patient information, from any source, he or she is not restricted by HIPAA in how the information is used or disclosed.

Conclusion

We urge policymakers to look at the substantial progress being made by doctors, hospitals, and health plans in implementing the medical privacy rule. Policymakers, as well as covered entities, should recognize that the HIPAA privacy rule will improve the quality of care and access to care by fostering patient trust and confidence in the health care system. People will be encouraged to more fully participate in their own care, and public health and research initiatives will benefit from more reliable patient data. Also, we urge HHS and the professional and trade associations to continue to focus resources on pursing an aggressive public education campaign that separates the Myths from the Facts. Once fully and fairly implemented, the HIPAA privacy regulation will improve the quality of health care and broaden access to health care services by bolstering patient trust and confidence in the health system.