Testimony of

Janlori Goldman, Director
Health Privacy Project, Georgetown University
Institute for Health Care Research and Policy

Before the

Senate Committee on Health, Education, Labor, and Pensions

On

“Making Patient Privacy a Reality:
Does the Final HHS Regulation Get the Job Done?”

February 8, 2001
Members of the Senate Committee on Health, Education, Labor, and Pensions:

As the Director of the Health Privacy Project at Georgetown University’s Institute for Health Care Research and Policy, I very much appreciate the invitation to testify before you today on the final medical privacy regulations.

Overview of HPP

The Health Privacy Project’s mission is to press for strong, workable privacy protections in the health care arena, with the goal of promoting increased access to care and improved quality of care. The Project conducts research and analysis on a wide range of health privacy issues. Recent Project publications include: Best Principles for Health Privacy (1999), which reflects the common ground achieved by a working group of diverse health care stakeholders; The State of Health Privacy (1999), the only comprehensive compilation of state health privacy statutes; Privacy and Confidentiality in Health Research (2000), commissioned by the National Bioethics Advisory Commission; Privacy and Health Websites, which found that the privacy policies and practices of 19 out of 21 sites were inadequate and misleading; and “Virtually Exposed: Privacy and E-Health” (2000), published in Health Affairs.

In addition, the Project staffs the Consumer Coalition for Health Privacy, comprised of over 100 of the major disability rights, disease, labor, and consumer advocates as well as health care provider groups. The Coalition’s Steering Committee includes AARP, American Nurses Association, Bazelon Center for Mental Health Law, National Association of People with AIDS, Genetic Alliance, Multiple Sclerosis Society, and National Partnership for Women & Families.

The Genesis of the Regulations

The new federal health privacy regulations are a major victory for all health care consumers. Each one of us will benefit from these rules in some way. The rules represent a
significant and decisive step toward restoring public trust in our nation's health care system. Not only is it the most sweeping privacy law in U.S. history, it begins to fill a most troubling vacuum in federal law. The regulation sets in place a sorely needed framework and a baseline on which to build. Much of the regulation's unfinished business is due to the legal constraints imposed on the Department of Health and Human Services by Congress in its delegation of authority in HIPAA. At this juncture, it is imperative that Congress acts to plug the gaps and strengthen the weaknesses in the rule.

In fact, it was the Congress that imposed on HHS the legal duty to issue health privacy regulations. In the 1996 Health Insurance Portability and Accountability Act (HIPAA), Congress imposed a deadline on itself to enact a comprehensive health privacy law within three years. Failure to meet the deadline triggered the requirement for HHS to promulgate rules in this area by 2000. Many bills were introduced, including by many members of this Committee. Some were bi-partisan; others were not. Some were favored by consumer advocates, others by health plans. Numerous hearings were held in both the House and this Committee, but not a single bill saw a mark-up. Achieving consensus on health privacy rules is not a simple task.

Pursuant to its mandate, HHS issued draft regulations in November 1999. In response to requests from industry representatives and consumer advocates, the Department extended the formal comment period to allow sufficient time to respond to the proposal. Of the 52,000 comments eventually submitted, more than half came from consumers and their representatives. The final regulation incorporates a number of the key changes sought by consumer groups as well as many of the changes urged by health care providers, health plans, clearinghouses, researchers, and others operating in the health care arena. It appears HHS was striving to craft a strong and workable privacy law.

It is important to note here that the privacy rule is one of three regulations mandated in the section of HIPAA known as “Administrative Simplification.” The other rules address establishing uniform transaction standards for health care and security rules to safeguard the data. Congress intended this package of regulations to be implemented together so that privacy
and security measures are built-in as information systems and practices are standardized. The policy goal was to assure the public that as their most sensitive personal information was being computerized and adapted to be shared instantly and cheaply, enforceable privacy rules were being implemented up-front.

**Privacy Is Central Value in Health Care**

In HIPAA's privacy mandate, Congress recognized that Americans are increasingly concerned about the loss of privacy in every-day life, and especially for their health information. The lack of privacy has led people to withdraw from full participation in their own health care because they are afraid that their most sensitive health records will fall into the wrong hands, and lead to discrimination, loss of benefits, stigma, and unwanted exposure. One out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information, including withholding information, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and — in the worst cases — avoiding care altogether. (Survey conducted by Princeton Survey Research Associates for the California Health Care Association, 1999)

Unfortunately, peoples' fears are warranted. Medical privacy breaches are reported with increasing frequency by the media. To highlight a few—

♦ Terri Seargent was fired from her job after her employer learned that she had been diagnosed with a genetic disorder that would require expensive treatment. Terri was a valued employee who received a positive review and a raise just before her discharge from the company. A recent EEOC investigation determined that the employer fired Terri because of her disability.

♦ A few months ago, 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.

♦ Annette W. and her husband were involved in a difficult and contentious divorce. In the midst of their separation, Annette instructed her pharmacy not to disclose any of her
medical information to her estranged husband. Just one day later, the pharmacist gave Annette’s husband a list of all her prescription drugs. Armed with this information, her husband embarked on a campaign to label her a drug user. He sent information to friends and family, to the Department of Motor Vehicles, and threatened to have her children taken away.

♦ Years ago, Ben Walker and his wife came to Congress and to this Committee to tell their story. Ben had worked for the FBI for 30 years, but was forced into early retirement after his employer learned that he had sought mental health treatment. The FBI got hold of Ben’s prescription drug records when the Bureau was investigating his therapist for fraud. In turn, the FBI targeted Ben as an unfit employee and stripped him of many of his duties, even though he was later found fit for employment. Ben and his wife testified that he would never have sought treatment had he believed his medical records would be used against him.

In the absence of a federal health privacy law, such as the one we have now, these people suffered job loss, loss of dignity, discrimination, and stigma. And had they acted on their fears and withdrawn from full participation in their own care – as nearly 20% of people do – they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have faced the untenable choice of shielding themselves from unwanted exposure or sharing openly with their health care providers.

Summary of Regulations

Key provisions of the health privacy regulation are highlighted below. Attached to this statement is a more detailed, comprehensive summary of the rule.

♦ **Scope:** The regulation applies all health care providers, health plans, and clearinghouses (entities that process and transmit claims data) that transmit health information in electronic form, and covers identifiable health information in electronic and paper records as well as oral communications. Due to the constraints imposed by HIPAA, the law does not directly cover employers, life insurers, pharmaceutical companies, and others. Instead, the rule establishes a chain of trust requirement, binding entities that receive identifiable health information from a covered entity to a contractual arrangement.

♦ **Access:** People have the right to see and copy their own medical records. Most states do not currently grant people such broad access.

♦ **Limits on Disclosure:** The regulation restricts access to and disclosure of health information. Of particular importance to patients and providers, health care providers
must obtain patient consent for disclosures relating to treatment, payment and health care operations. However, we believe the sections on marketing and fund-raising are fundamentally flawed in allowing “one free pass” before first giving people the chance to opt-out of receiving such communications.

♦ **Employers:** Employers are barred from receiving “protected health information” except for specific functions related to providing and paying for health care. Employers must establish a firewall between the health care division and employees who make decisions about employment. The rules are a powerful new tool to stop workplace discrimination. However, due to constraints imposed by HIPAA, employers that collect health information directly from employees (and not in their capacity as providers, plans or clearinghouses) fall outside the scope of the privacy rule, because the regulation cannot directly cover employers. This gap should be closed.

♦ **Law Enforcement:** Health care providers and plans are prohibited from releasing patient data to federal, state, or local law enforcement without some form of legal process, including a warrant, court order or administrative subpoena. But the legal process requirements should be strengthened to require a higher Fourth-Amendment standard and review by a neutral magistrate.

♦ **Research:** All research, whether publicly or privately funded, must be overseen by either an Institutional Review Board (IRB) or privacy board if the researcher seeks a waiver of informed consent.

♦ **Penalties:** Health care providers, health plans, and clearinghouses are subject to civil and criminal penalties (up to $250,000/year and 10 years in jail) for violating the law. The Office for Civil Rights at HHS is charged with overseeing the law and imposing penalties where appropriate. But HIPAA constrained the Secretary from including a private right of action for individuals to sue for violations of the law. Congress should act to give people the ability to seek redress directly if their rights are violated.

♦ **Preemption:** As required in HIPAA, the federal regulation does not preempt or override stronger state law. Instead, the rules establish a baseline of protections, above which states may go to better protect their citizens. A 1999 report issued by the Health Privacy Project demonstrated that such a baseline is sorely needed.

♦ **Cost:** Government estimates that the cost associated with implementing the privacy regulation (approximately $17 billion over 10 years) will be greatly offset by the cost savings associated with implementing HIPAA’s transaction standards (approximately $29 billion saved over 10 years). Again, if implemented together as contemplated by Congress, consumers will benefit, health care organizations will benefit, and the health of our communities will benefit.

**Conclusion**

In conclusion, Americans should be proud by what Congress set in motion with HIPAA. Health care providers, plans, and clearinghouses should focus their resources in the coming
years on implementing the HIPAA regulations, thereby improving health care quality and access, while also protecting privacy. At the same time, we urge this Congress to:

1. broaden HIPAA’s scope to directly cover other entities that collect and use personal health information;
2. require consumer consent before medical information can be used for marketing and fund-raising;
3. strengthen the limits on law enforcement access to medical records; and
4. equip people with the right to go to court if their privacy is violated under the law.

We look forward to continued progress on health privacy. Our health care system has changed dramatically in the last few years, bringing with it both promise and perils. We have mapped the human genome, but people are afraid to get tested. The Internet can deliver cutting edge research and health care services, but people are unwilling to trust their most sensitive information in cyberspace. We will never fully reap the benefits of these astounding breakthroughs until privacy is woven into the fabric of our nation’s health care system.