ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003 **www.bobgellman.com**

Statement of Robert Gellman

Presented to the Subcommittee on Privacy and Confidentiality
National Committee on Vital and Health Statistics

Hearing on Approaches to Studying the HIPAA Privacy Rule

November 30, 2006

Let me begin with a brief introduction. I am a privacy and information policy consultant in Washington, DC. I am here representing myself. My clients have included federal agencies, large and small companies, trade associations, non-profits, and foreign governments. I have no current clients in the health policy space.

I am not a privacy advocate, but I do work with privacy advocates from time to time. Recently, I have been working on some health information issues with the World Privacy Forum.

For seventeen years ending in 1995, I worked on the staff of a subcommittee of the Committee on Government Operations in the House of Representatives. My responsibilities included privacy, freedom of information, and other information policy matters. During 1979-80 and again in 1993-94, I was the lead House staffer on health privacy legislation. Both efforts resulting in bills that moved through committee but did not become law.

I served as a member of the National Committee on Vital and Health Statistics from 1996-2000. I was chair of the privacy and confidentiality subcommittee for part of that time.

I have three broad points that I want to offer to the committee.

First, too often, those looking at health data issues see privacy as an impediment to some other goal. Borrowing a line from the software industry, let me assert that privacy isn't a bug. It's a feature. Privacy is not a barrier. It is an essential part of health care, and it has been since the days of Hippocrates. Privacy is not an impediment. Patient privacy expectations must be recognized, along with the other competing objectives of high-quality health care, low cost health care, and health care for all.

Unfortunately, privacy continues to take a backseat at the policy level. A metaphor for privacy is the guy with the broom following the circus parade. Let's decide where we are going and then, as an afterthought, consider how to make privacy fit in with decisions already made. That is the wrong approach. We cannot let the data enthusiasts alone direct the network parade. Consumers must be allowed to participate effectively in the decision making process.

We do not need to study the value of privacy. The principles of privacy as reflected in Fair Information Practices promote basic rights that must be incorporated in the health care system. Replowing this ground is a waste of time and effort, although it is fair to ask if we are addressing privacy in an effective and efficient way.

My first point then is that privacy must be accepted as a basic part of health care. That is a starting point. Privacy must be adequately considered when policy choices are made and consumers must be part of that policy process.

Second, what might we study about health privacy? Should we inquire if patients know what their rights are under HIPAA? Frankly, I don't see that question as having any priority at all. I agree that it would be nice if more patients knew that they had rights of access and correction. But it is much more important that those within the health care system know what their obligations are. Patients will catch up in due course. And they will surely catch up at the time when it makes a difference to them.

Let me make this point another way. How many people in this room know what their rights are under Gramm-Leach-Bliley? Or the Privacy Act of 1974? Or the Fair and Accurate Credit Transactions Act? I believe that the answer is not very many. My point is that we should not assess patient awareness against a standard that many smart and knowledgeable people can't meet for other comparable laws. Don't hold the health care sector to a standard that no other sector meets. Informing consumers about privacy rights is helpful, but it is more important that the rights exist.

Should we want to know about the costs to the health care system of implementing HIPAA? I don't see that as particularly important. HIPAA made providers and insurers do what they should have been doing anyway. Any health care institution that already had a reasonable privacy policy could have implemented the HIPAA privacy rule with little cost or effort. How many hospitals had a privacy policy before HIPAA? How many trained their staff in privacy? Few health care institutions paid much active attention to privacy before HIPAA. Privacy received lip service, but nothing else. The marginal cost of HIPAA over what *should* have been done is a small meaningless number.

My second point then is that focusing on privacy knowledge or costs will not be productive. Paying attention to implementation by covered entities may yield some insights, but don't be distracted by privacy matters that are not relevant.

Third, like it or not, the HIPAA privacy rule is yesterday's policy. Think about how far the Internet has evolved since HHS first started drafting the HIPAA rule in the 1990s. We will be living in a digitized and networked environment in the future. I don't know whether that is good or bad because I don't know what a health information network will do, how much it will cost, who will pay for it, and what the real benefits are. But it seems likely that we will end up with some kind of health network somehow.

Much of the policy reflected in HIPAA is geared to the paper world. The privacy rule won't work in the same way in a networked environment. HIPAA did some good things, but it is

nevertheless filled with problems and poor policy choices. The current rule is probably beyond repair for administrative and political reasons. We do not need to study how to perfect the buggy whip. This committee should mostly focus its attention beyond HIPAA.

A network will enhance data use, but it can also enhance privacy rights too. In a networked environment, patients who care to exercise more control over their health information could do so because a practical and cost-effective way can be built into the network. New technology can enhance patient rights to access and correct records. The restrictions (including, but not limited to, the exclusion of third party information from correction) on these rights in HIPAA will not work. New technology can allow for the accounting of every use and disclosure of health records at little cost. The restrictions on these obligations in HIPAA will not work and are inappropriate in a networked environment. New technology can allow patients to participate in and receive actual notice of uses and disclosures of their health records for public health, research, and other activities. The HIPAA policy that patients have no effective right to restrict use and disclosure will not work anymore.

The committee should look at how new technology will force more tradeoffs between privacy, other goals, and existing institutions. Here is an example. We use institutional review boards to decide if research outweighs privacy interests. Whether IRBs work well or not, they represent a practical approach to balancing competing goals in a paper-based world. In a networked environment, we have the capacity to allow each individual patient to strike a balance for the use of his or her own record in research. The technology will manage everything in a cost-effective manner, and we will no longer need IRBs for that purpose. IRBs will continue to have other roles. The network will allow a significant reconceptualization of the balancing of interests.

My third point then is that we need to look far beyond HIPAA and determine how technology will change the way that health data is used and should affect the rights of data subjects. Here are some potential areas of study that I think would be valuable for the Subcommittee and the Department to pursue:

1. Medical Identity Theft.

Medical identity theft occurs when someone uses an individual's name or other parts of the individual's identity – such as insurance information or Social Security Number – without the victim's knowledge or consent in order to obtain medical services or goods. Medical identity theft can also occur when someone uses an individual's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims. The essence of the crime is the use of a medical identity by a criminal and the lack of knowledge by the victim. We do not know how many medical identity theft victims exist, but the best estimate is between a quarter of a million and half a million in 2003.

The World Privacy Forum published a report on medical identity theft earlier this year. You can find the report, *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You*, at the WPF Medical Identity Theft page. <http://www.worldprivacyforum.org/medicalidentitytheft.html>. I was a small contributor to the

report, but Pam Dixon of the WPF deserves all of the credit for the original research and for bringing this problem to public attention.

A health information network is an identity thief's dream. It could contain the names, numbers, and other detailed information about nearly everyone in the United States. Millions of people in the health care sector could have legitimate access to a network. If only one person in a hundred thousand is a crook, then more than one thousand crooks could be surfing the network from inside every day. If we do not control medical identity theft, efforts at networking will fail miserably. A few horror stories will have patients and politicians running for the exits.

We need to know more about the nature, scope, and consequences of medical identity theft. We need to know how to adjust privacy rules to meet the needs of victims. For victims seeking to recover from medical identity theft, the current HIPAA rules hurt more than they help. Limits on access and correction rights can defeat legitimate efforts by victims to remove erroneous information from their health records.

In an appendix to this testimony, I suggest some of the information that should be collected in order to obtaining a better understanding of medical identity theft and of how to adjust the health record system to meet the needs of victims.

2. Health Scores

Any type of health network is likely to facilitate the development of health scores for consumers just like the credit reporting system currently supports the use of credit scores. When credit reporting became centralized, national in scope, and universal, no one foresaw the development of credit scores. But we have them now, and the scores are widely used throughout the economy. Those with low scores or with no scores face greater difficulties in navigating through the economy.

The centralization of information about health will allow for the development of new measures about the health of individuals or families that might be used by employers, credit grantors, auto insurers, landlords, colleges, marketers, and others who make decisions about how people can work, live, shop, or function generally in society.

A health score might utilize a single number to predict the costs that an individual or a family would impose on the health care system in the next year or two. Other health scores might be calculated to assess how likely an individual is to show up at work or school, buy health related products, or make other choices. Advances in genetics may open the door to scoring the genetic heritage of individuals and families. Health scores could affect or even determine the future of an individual by opening or foreclosing opportunities for education, places to live, insurance, employment, or credit.

I know little about the extent to which health scores are being utilized today. The best example comes from Medicaid, which uses resource utilization groups (RUG) to classify residents in nursing homes based on the relative resources that an individual is likely to use.

It would be useful to know whether more health scores are being used elsewhere today by the government or by the private sector. Any shared health information resource could easily be used to calculate a health score with the potential for undesirable and potentially uncontrollable consequences.

A broader point is that we need to study the effects of impending health information technology developments on privacy and on people. We need to think outside the current box and to look as far into the future as possible. We need to anticipate the possibilities and make appropriate decisions about what we should allow and what we should seek to prevent.

3. Surveillance System

A health network has the potential to be a general surveillance system. This is another example of how a health network can create broader problems that receive no attention from data enthusiasts who want unlimited patient data for their own purposes. It is not unlikely that a network will include information about appointments. The idea is to see your doctor and also schedule appointments with other providers through the network all at one time.

Now remember that HIPAA grants the police virtually unlimited access to health records without a warrant, without a subpoena, and without a written request. It's called an administrative request [45 CFR §164.512(f)(1)(ii)(C)]. A law enforcement official need only make three specific oral representations in order to qualify to obtain information. Further, some police agencies are likely to have direct access to a health network for health care fraud or other legitimate investigatory purposes.

A health network operating under these rules is a surveillance system for the police. If you are wanted by government because of an outstanding arrest warrant, tax debt, questionable immigration status, suspicion of terrorism, overdue library book, or some other reason, every medical appointment would put you in jeopardy. The police could run their list of wanted individuals through the network and arrest, detain, or question people who show up for appointments the next day.

I suggest that a health information system that includes this possibility may need some study and some new limits. It will only take a handful of horror stories for a health information network to be seen as a tool of Big Brother.

4. Preemption

The HIPAA statute mandates that stronger state laws trump the federal health privacy rule. That was the right policy at the time of passage. In a networked environment, a patchwork quilt of laws is mostly impractical in my judgment, although some in the privacy community still favor stronger state laws. Network enthusiasts want complete federal preemption.

In my opinion, the only outcome more complex than today's patchwork quilt of state laws is a federal law that occupies the field and preempts every state law. An expansively preemptive federal law would affect dozens or hundreds of laws in each state. The result would

be chaos. Existing institutions and activities would freeze. It would take years for states to revise their codes to reflect their new, limited authority in the health information arena. Federal regulations would have to be ten times longer than the HIPAA privacy rule. Simplification of health privacy laws by total federal preemption is a myth.

I believe that neither extreme – full federal preemption on the one hand and stronger state law preemption on the other – will be practical in the future. This committee could usefully begin the hard work of finding a workable middle ground that would deal with the need for more uniformity while recognizing structural legislation that exists in the states and accommodating the widespread legislative recognition that some health information legitimately requires different treatment. Existing laws protecting psychiatric, substance abuse, HIV, and genetic information are not likely to be wiped out entirely to satisfy lazy health network designers.

***

If I have a general conclusion, it is that if you fail to satisfy the public demand for health privacy, then the public will upset the march toward health record digitization and the ever-increasing demands for sharing of health data. The problems are great, the conflicts are sharp, and solutions will only be found if all of the stakeholders – especially including consumers – are involved in the process. This committee can help by taking a dispassionate and objective look at issues that truly need attention.

Thank you for the opportunity to appear at this hearing.

Appendix: Outline for a Study of Medical Identity Theft

A study of medical identity theft should:

· Propose one or more definitions of medical identity theft. The study should also compare and contrast medical identity theft with financial identity theft. However, except as a definitional matter or as otherwise expressly relevant to medical identity theft, the study should avoid delving far into financial identity theft. For example, if a clerk in a hospital steals a patient's information and uses it to obtain a credit card in the patient's name, that activity is financial identity theft that happened to originate in the health care system and is not directly relevant to this request.

· Estimate the number of medical identity theft victims and the number of medical identity theft incidents. Not all cases of medical identity theft occur in the name of an innocent individual. The study should also seek to estimate the cost of medical identity theft to victims, insurers, providers, and others.

· Evaluate the incidence of medical identity theft for health professionals. In this type of medical identity theft, the criminal assumes the identity of a health professional in order to make claims for services never provided. There may be various forms of this type of medical identity theft, and the study should identify all methods used by criminals who assume the identity of a health professional.

· Determine the extent to which the Department of Health and Human Services is aware of medical identity theft and whether the privacy and security rules issues under the authority of the Health Insurance Portability and Accountability Act are sensitive to and helpful to the needs of medical identity theft.

· Determine the extent of awareness of medical identity theft among health insurers and health care providers. The study should report on and assess actions taken by insurers and providers to prevent, avoid, or detect medical identity theft.

· Seek to identity any patterns for medical identity theft. For example, are large providers or small providers more likely to be targets? Are federal insurance programs more likely or less likely to be targets? Is there a noteworthy geographical distribution to medical identity theft activities? Are young or old people more likely to be victims?

· Determine the extent to which computerization of health information, electronic health transactions, and health networks help or hurt in the detection and prevention of medical identity theft. In particular, the study should attempt to assess whether planners for a national health information network are taking medical identity theft into account when developing the architecture and operations of the network.

· Collect and report on incidents of medical identity theft, including case studies that show how individual victims learn about, respond to, and recover from medical identity theft. It may be useful here to compare and contrast remedies for victims of financial identity theft with remedies for victims of medical identity theft.

· Report on any private or government litigation that arises out of medical identity theft. Government litigation may include civil or criminal actions against medical identity thieves. Private litigation brought by victims of medical identity theft against health care providers and health insurers is also of particular interest. In addition to any statistics on litigation, it would be useful to have case studies of litigation brought by victims.

· Make recommendations to the Congress, the President, the Department of Health and Human Services, health care providers, health insurers, and others for responding to medical identity theft. In particular, recommendations for changes in law or regulations that would benefit individual victims of medical identity theft would be welcome.

*****