IDEAS ON LIBERTY
OCTOBER 2002

The Peril to Our Privacy

by Sue A. Blevins

If the Bush administration has its way, beginning in April 2003 individuals' personal health information—including genetic information—will be shared with data-processing companies, insurance companies, doctors, hospitals, researchers, and others *without* their consent. This is a major shift from today's standard whereby patients give their consent before their medical records are shared with third parties. The administration proposes to eliminate the current standard in order to make processing medical claims more efficient. If the changes are adopted, every American will have effectively lost any ability to maintain a confidential doctor-patient relationship.

How did the federal medical privacy rule come about? Who was behind it? What can Americans do to protect their medical privacy?

Until now, health privacy was considered a matter regulated by the states. Every state has a law to protect citizens' medical records. However, abiding by 50 different state privacy laws has proved difficult for the industries that want to create a national health-information system. National leaders of the medical, hospital, health-insurance, and other industries have been working for over a decade to nationalize standards for electronic claims processing. In 1991 the Workgroup for Electronic Data Interchange (WEDI) was established to lobby Congress for legislation to enable electronic medical records and payment systems.

WEDI was instrumental in getting many of its goals incorporated into the infamous Clinton health-care plan. President Clinton's 1993 Health Security Plan included a provision titled "Administrative Simplification." It called for establishing a national health-information infrastructure, requiring unique identifiers to be assigned to four groups for processing medical claims electronically: every (1) health-care provider, (2) health plan, (3) employer, and (4) individual. The Administrative Simplification plan also called for creating uniform national codes for medical claims and for establishing federal medical privacy rules. The bottom line is that you can't create a national health-care system without standardized information.

Congress and the American people vehemently rejected the Clinton plan to nationalize health care. However, the Administrative Simplification provision was tucked away in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which was signed into law on August 21, 1996 (Public Law 104–191). Many remember HIPAA as the legislation that was supposed to make health insurance portable and affordable. (It never met those purported goals.) Under HIPAA, the same four groups mentioned above would be required to have unique identifiers for processing claims elec-

Sue Blevins (sblevins@ForHealthFreedom.org) is president of the Institute for Health Freedom in Washington, D.C. (www.ForHealthFreedom.org).

tronically. Thanks to the diligent work of U.S. Representative Ron Paul, federal funding for a health-identifier system has been put on hold over the past few years. But unless that provision of the HIPAA statute is repealed, all Americans may soon be assigned a number for tracking their medical information from cradle to grave.

Aware that the American people were concerned about medical privacy, legislators included a provision in HIPAA requiring that a medical-privacy law be passed by August 21, 1999, or the secretary of Health and Human Services (HHS) would have to generate such a rule. HIPAA also included a provision that gave WEDI (and other groups) legislative authority to advise HHS on the forthcoming national health-information system and medical privacy. Congress missed its self-imposed deadline, and the authority to establish federal regulations for medical privacy shifted to the Clinton administration.

Clinton Administration Rule

In November 1999 the Clinton administration proposed federal regulations relating to medical privacy. They would have *prohibited* doctors, hospitals, and others from obtaining patients' consent before releasing their medical information. However, the public spoke out against the rule. HHS received more than 52,000 comments during the public comment period. The issue most discussed was patient control of personal health information.

A final federal medical privacy rule was published in December 2000, just before President Clinton's departure. It prohibited release without consent of information for treatment, payment, or "health care operations"—a broad term encompassing many activities. However, many other third parties did not need patients' consent before obtaining their medical records. These included law-enforcement officials, researchers, public-health officials, and many more.

The medical and insurance industries were strongly opposed to the consent provision as it appeared in the final rule. They lobbied the incoming administration strongly to eliminate it. Not surprisingly, in March 2002 the Bush administration proposed to modify the rule so that health-care insurers, providers, institutions, and others could transfer medical information electronically to pay claims, treat patients, and do other tasks—without patients' consent. Instead, the Bush administration called for providers simply to notify patients about how their information is being shared. It will complete the revisions in the coming months.

In essence, the federal government is giving the medical industry regulatory authority to decide whether personal health information can be obtained by others without patients' permission. What's more, WEDI and other medical-industry groups strongly support pre-empting state laws regarding medical privacy. Given their strong lobbying success, it is likely that in the near future state laws will be replaced by the federal medical-privacy rule. This will be a large leap toward national health care.

The privacy rule is one of the greatest infringements on liberty that this country has ever experienced. It applies to all citizens, whether they rely on government assistance or pay privately for their health care. As written and soon to be enforced, the rule requires doctors, therapists, and other providers to share patients' health-related information—including psychotherapy notes—with the secretary of HHS. The government's rationale is that federal agents need to invade your privacy to protect it.

The only way that citizens will be able to maintain their medical privacy in coming years is to have private contracts with doctors and other health-care providers. It is not clear whether the current version of the privacy rule will interfere with an individual's right to make contracts. But what is clear is that every American is losing the freedom to maintain a confidential doctor-patient relationship. □

IDEAS ON LIBERTY
OCTOBER 2002

The Danger of National Identification

by David M. Brown

It seems innocuous. What could be so sinister about finding out who people are? But the national identification regime that some in government and the media want to establish in response to the September 11 terrorist attacks would likely do much to threaten individual privacy and security while doing little in itself to prevent terrorism.

There are many different ID proposals floating around, but a full-fledged national ID system would impose a mandatory identification card for all citizens and residents of the nation. In *The Limits of Privacy,* Amitai Etzioni, an enthusiast for this and other forms of round-the-clock surveillance of innocent people, describes national ID cards as "domestic passport-like documents that citizens of many countries, including democracies, are required to have with them at all times."

Etzioni states that such a card has three characteristics: (1) all citizens and residents "of a given jurisdiction" must have it; (2) all must carry it and present it on request by authorities; (3) each card must be linked to a database with other information about the person. "Note that presenting such identification is required even when there is no specific evidence that a crime has been committed or a regulation violated," he explains. Most current proposals tout the benefits of linking the cardholder to a national database. The proposals vary only with respect to what kind of information is to be included in the database, which would aggregate and combine data from sundry existing databases.

Many proponents of the proposed "trusted traveler card" for airline passengers would like every possible kind of information about you to be included in the database, everything from your criminal record to how you bought your tickets to your travel record. The more information that is collected, the more robust will be the profile that is constructed. The purpose of the profile would not merely be to flag those with a violent criminal record who are on the run from the law. It also would be to predict how likely a terrorist threat you are based on such factors as how you bought your ticket and whether your name is Arabic or Anglo-Saxon. The implicit premise is that no one can be secure unless everyone is treated as a criminal suspect.

The United States already has experience with schemes of universal or quasi-universal identification. The Social Security number, often in conjunction with the state-issued driver's license, has become a kind of de facto universal identifier, even though its originally stated purpose was merely to log the so-called contributions of Social Security participants. For many years the Social Secu-

David Brown (dmb1000@juno.com) is the publisher of The Crunch Report *(www.thecrunchreport.com), a webzine. He helped develop the I Am Not a Number Campaign for the Bureaucrash website.*