



February 1, 2007

John O. Agwunobi, Assistant Secretary for Health
Office of Public Health and Science
Attention: Personalized Health Care RFI
Department of Health and Human Services
200 Independence Avenue, SW, Room 434E
Washington, DC 20201

Re: Request for Information (RFI): Improving Health and Accelerating Personalized Health Care through Health Information Technology and Genomic Information in Population and Community-Based Health Care Delivery Systems

Dear Mr. Agwunobi:

This letter serves to share important public comments regarding the U.S. Department of Health and Human Services' (HHS) "Request for Information (RFI): Improving Health and Accelerating Personalized Health Care through Health Information Technology and Genomic Information in Population and Community-Based Health Care Delivery Systems."¹

HHS's public notice states: "Input is sought on the interest and current planning activities of health care systems and related organizations on the needs and applications of these transformative aspects of personalized health care. Specific areas for comment include...Organizational or institutional practices to address *ethical, legal, and social implications regarding the use of patient information, including genetic data*, to support personalized health care." [Emphasis added.] Regarding this topic, it is important for HHS, and those promoting interoperable electronic medical records, to acknowledge this important fact: Simplifying the transfer of electronic health information *also* makes it easier to share individuals' personal health data *without* their consent, thereby weakening citizens' health-privacy rights.

Public Concerns

According to psychiatrist and privacy advocate Deborah C. Peel, M.D., if people believe that their health information is *not* going to be kept confidential (between the individual and his or her physician/other health-care provider) then many individuals often lie or avoid sharing critical information. (One can only imagine how seriously this must distort medical data that is used for research studies and public health purposes.) In fact, a national survey conducted by Forrester Research in 2005 for the California HealthCare Foundation found that nearly one out of eight (13 percent) of respondents report having engaged in one or more of the following privacy-protection behaviors:

- Asked a doctor not to record a health problem, or record a less-serious/embarrassing diagnosis.
- Gone to another doctor to avoid telling their regular MD about a health condition.
- Personally paid for a test, procedure, or counseling rather than submit a claim, out of concern someone else would access the information.
- Decided not to be tested, out of concern that others might find out the results.²

The survey also found that 67 percent of respondents are concerned about the confidentiality of their medical records, although the same percentage is “aware of federal laws that protect the privacy and confidentiality” of those records. Thus even though a majority of Americans are aware of the Federal Medical-Privacy Rule, most don’t believe it accomplishes what it promises.

Currently, many Americans are concerned about losing control over their personal health privacy with the shift toward electronic health records (EHRs). In fact, Americans’ top concern about EHRs is the potential misuse of their personal data, according to a recent national survey conducted on behalf of the Markle Foundation.³ Eighty percent of respondents said they would be *very concerned* about identity theft/fraud if an online network provided people with access to their medical information.

Are their concerns unfounded? Consider just a small sample of excerpts from recent newspaper articles regarding health-privacy and data-security issues:

- “While some describe electronic medical records as a superhighway to better care and increased efficiency in the medical system, others worry that it could be a dangerous dark alley. ‘The electronic health system is not safe,’ said Deborah C. Peel, an Austin, Texas, psychiatrist who founded the Patient Privacy Rights Foundation. Just ask David Richardson. An acquaintance of Richardson’s used the Philadelphia man’s name and health insurance information to obtain medical services at several hospitals, according to the Pennsylvania Attorney General’s Office. The plot unraveled when Richardson’s insurance company, Aetna, contacted Richardson and asked him about the services. Investigators tracked down the imposter, Daniel Sullivan, also of Philadelphia. ‘One of the big concerns we have about medical identity theft is that it may compromise the victim’s medical history if the medical information of the thief gets merged with the victim’s medical history,’ said Nils Frederiksen, spokesman for the Pennsylvania Attorney General’s Office, which handled the case. For example, the victim and the thief may have different reactions to drugs, such as penicillin. ‘There is also a potential for more medical identity theft, just as there is a potential for more credit card theft, because of the ease of the electronic transfer of information or because of electronic databases that might be compromised,’ he said.” Source: “Electronic Medical Data Less Than Secure,” *Philadelphia Inquirer*, January 30, 2007.

- “Computer records containing medical claim information, health data and Social Security numbers of 28,279 health insurance customers of Nationwide Mutual Insurance Co. were stolen from the office of a vendor in Massachusetts, the company said. A lockbox that contained computer backup tapes with information on Nationwide Health Plan customers was taken during an Oct. 26 break-in at Concentra Preferred Systems in Weymouth, Mass., Columbus-based Nationwide said. In that theft, backup tapes of medical claim data of about 130,000 Aetna Inc. health insurance members also were taken, Aetna said in December. Nationwide’s health insurance unit hires Concentra to audit hospital-stay charges.” Source: “Data on Nationwide Insurance Stolen,” Associated Press (*Washington Post.com*), January 24, 2007.
- “When Lind Weaver opened her mailbox one day in early 2004, she was surprised to find a bill from a local hospital for the amputation of her right foot. Surprised because the 57-year-old owner of a horse farm in Palm Coast, Fla., had never had worse than an ingrown toenail. After weeks of wrangling with the hospital’s billing reps, Weaver finally stormed into the facility and kicked her heels up on the desk of the chief administrator. ‘Obviously, I have both of my feet,’ she told him.... Weaver’s identity had been stolen by a fraudster who had used her personal information—her address, Social Security number, and even her insurance ID number—to have the expensive procedure performed. The nightmare didn’t end there. When Weaver was hospitalized a year later for a hysterectomy, she realized the amputee’s medical info was now mixed in with her own after a nurse reviewed her chart and said, ‘I see you have diabetes.’ (She doesn’t.) With medical data expected to begin flowing more freely among health-care providers, Weaver now frets that if she is ever rushed to a hospital, she could receive improper care—a transfusion with the wrong type of blood, for instance, or a medicine to which she’s allergic. ‘I now live in fear that if something ever happened to me, I could get the wrong kind of medical treatment,’ she says.... Even worse, it can be difficult for patients to purge any fraud from their records. While the Fair Credit Reporting Act gives victims of financial identity theft the right to see and try to correct any mistakes in their credit records, critics say that victims of medical ID theft don’t have the same recourse. Health privacy laws ‘are limited and don’t reflect the possibility of medical ID theft,’ notes Robert Gellman, a leading privacy consultant in Washington. ‘Negative information could just bounce around the system forever.’... Law enforcement authorities complain that many health-care facilities do too little to protect their patient data. Case in point: In September, federal authorities arrested a scheduling clerk at the Cleveland Clinic’s Weston (Fla.) hospital who allegedly had passed on the personal identification information of more than 1,100 patients to her cousin—who in turn submitted \$2.8 million in false claims to Medicare. ‘Hospitals have done a poor job of implementing security procedures on their computer systems,’ says one federal investigator. ‘You’d be astonished how many people have access to your medical records.’” Source: “Diagnosis: Identity Theft,” *BusinessWeek*, January 8, 2007.

- “Security weaknesses have left millions of elderly, disabled and poor Americans vulnerable to unauthorized disclosure of their medical and personal records, federal investigators said Tuesday. The Government Accountability Office said it discovered 47 weaknesses in the computer system used by the Centers for Medicare and Medicaid Services to send and receive bills and to communicate with health care providers. The agency oversees health care programs that benefit one in every four Americans. Its massive amount of data is transmitted through a computer network that is privately owned and operated. However, CMS did not always ensure that its contractor followed the agency’s security policies and standards, according to the GAO report. ‘As a result, sensitive, personally identifiable medical data traversing this network are vulnerable to unauthorized disclosure,’ the federal investigators said. The network handling Medicare claims transmits extremely personal information, such as a patient’s diagnosis, the types of drugs the patient takes, plus the type of treatment facility they visited, including treatment centers for substance abuse or mental illness.” Source: Health Privacy Project (www.healthprivacy.org), citing “Auditors: Health Records at Risk,” Associated Press, October 3, 2006.
- “Over the past three years, millions of Americans visiting doctors’ offices, pharmacies and hospitals have been handed forms and brochures discussing privacy rules under the Health Insurance Portability and Accountability Act, or HIPAA. Many assume signing somehow protects their privacy. It doesn’t. In fact, the disclosure notice essentially details the many ways a doctor can use and disclose medical information—often without a patient’s consent or knowledge. Medical providers have to ask for a signature. But signing isn’t mandatory. And failing to sign usually doesn’t change what a doctor can and can’t do with a person’s medical information....Health plans and medical providers also must track some kinds of disclosures, and give patients a list if asked, including disclosures for public-health purposes, but not routine uses for treatment, payment or health-care operations....The privacy rules also give patients the right to ask for additional restrictions on who can see their records and why.... However, providers don’t have to agree in the first place—at least under federal law. And some health plans and medical providers, especially large ones, make it a policy not to grant special restrictions, saying it’s too complicated.” Source: “Taking Control: Setting the Records Straight,” *Wall Street Journal*, October 21, 2006.

Genetic Privacy and Public Opinion

The Institute for Health Freedom (IHF) commissioned a national Gallup survey (in 2000) to find out how Americans feel about medical and genetic privacy.⁴ IHF is a nonprofit, nonpartisan educational organization (a think tank) founded in 1996 to bring the issues of personal health freedom to the forefront of America’s health-policy debate. Our mission is to present the ethical and economic case for strengthening personal “health freedom,” defined as:

The freedom to choose one's health care providers and treatments, and to maintain confidential relationships with one's providers, without interference from government or private third parties.

To this end, we had heard from privacy advocates across the country about their concerns over health privacy issues. But we wanted to find out how ordinary citizens across the nation felt about the issue. The national Gallup survey results show that an overwhelming majority of Americans do not want the government or other third parties to have access to their medical records—including genetic information—without their permission. The survey of 1,000 adults nationwide found that 78 percent say it is very important that their medical records be kept confidential. According to a majority of respondents, no third party should be permitted to see their records without permission. Key findings include:

- 92 percent oppose allowing governmental agencies access to patients' medical records without permission;
- 88 percent oppose letting police or lawyers review medical records without explicit consent;
- 84 percent say employers should not be allowed access to patients' medical records without permission;
- 82 percent object to insurance companies gaining access without permission;
- 71 percent oppose giving doctors (*other than* the ones given permission by the respondent) access to their medical records without permission; and
- 67 percent oppose researchers accessing patients' medical records without consent.

The national Gallup survey also included two important questions about genetic privacy:

- One asked whether doctors should be allowed to test patients for genetic factors without their consent. Only 14 percent of respondents would permit such testing; 86 percent oppose it.
- The other question asked whether medical and governmental researchers should be allowed to study individuals' genetic information without first obtaining their permission. More than nine in ten adults (93%) feel medical and governmental researchers should first obtain permission before studying their genetic information.

Recommendations: HHS Action Needed to Address Public Concerns about Medical and Genetic Privacy

As the nation's largest single payer of health care, HHS should make sure the following ethical and legal rights are afforded to *all* Americans. These rights can be ensured *if* HHS acts to make sure every health-care provider and/or institution that receives government payments (taxpayer funds) upholds the following ethics and privacy rights:

- Right to Health Privacy: Individuals' personal health information should *not* be shared without individuals' fully informed written consent. The HIPAA-

mandated Federal Medical Privacy Rule does *not* ensure this ethic or right; thus the rule should be repealed or modified to ensure true health-privacy rights.

- Ownership of Personal Health Information, Including Genetic Information: Individuals must be ensured the ethical and legal right to own their personal health information, including genetic information and electronic health records (EHRs).

Public opinion polls show that Americans deeply value health privacy—and expect it! Thus, our nation’s government health agency should reflect the will of the people in upholding this precious freedom, as well as the legal right to ownership of health information (including genetic information).

Thank you for your attention to this important national issue.

Sincerely,



Sue A. Blevins
President

¹ “Request for Information (RFI): Improving Health and Accelerating Personalized Health Care Through Health Information Technology and Genomic Information in Population and Community-Based Health Care Delivery Systems,” *Federal Register* (Vol. 71, No. 211), November 1, 2006, pp. 64282-4; and *Federal Register* (Vol. 71, No. 239), December 13, 2006, p. 74914 (re: extension of comment period).

² “National Consumer Health Privacy Survey 2005,” California HealthCare Foundation (<http://www.chcf.org/topics/view.cfm?itemID=115694>).

³ “Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care,” Markle Foundation, December 7, 2006.

⁴ The Gallup survey, titled “Public Attitudes toward Medical Privacy,” was conducted by telephone with 1,000 adults nationwide between August 11 and August 26, 2000. The margin of error is plus or minus 3 percent. The survey report can be viewed in its entirety at the Institute for Health Freedom’s Web site (www.forhealthfreedom.org/Gallupsurvey).