WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum
Regarding
The U.S. Department of Health and Human Service Personalized Health Care
Request For Information

February 5, 2007

Office of the Secretary
U.S. Department of Health and Human Service
Room 434E
200 Independence Avenue S.W.,
Washington, D.C. 20201, Attention: Personalized Health Care RFI

VIA PHCRFI@hhs.gov

> **Re: The U.S. Department of Health and Human Service Request For Information: Improving Health and Accelerating Personalized Health Care Through Health Information Technology and Genomic Information in Population- and Community-Based Health Care Delivery Systems, 71 Fed. Reg. 64282-84 (Nov. 1, 2006).**

The Department of Health and Human Services has requested information regarding personalized medicine in a request for information (RFI) published November 1, 2006 in the Federal Register.[1]

The RFI states:

> For the purpose of achieving a broader understanding of rapid changes occurring in the health care setting that may have an impact on the future of personalized health care, HHS requests input from the public and private sectors on plans for developing and using resources involving health information technology (IT) and genetic and molecular medicine, with specific reference to incorporating these capacities in evidence-based clinical practice, health outcomes evaluations, and research.[2]

The request for information was broad and unspecific, which limits our ability to provide explicit advice regarding any specific projects. Our comments therefore address the

---

[1] 71 Fed. Reg. 64282-84 (Nov. 1, 2006).

[2] *Ibid*. See also <http://www.aspe.hhs.gov/PHC/rfi/v11.cfm>.

subject at a high level of generality. However, these comments will still be generalizable to specific projects formed as part of efforts resulting from this RFI. The World Privacy Forum is a non-partisan, non-profit public interest research organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to health care. One recent WPF research report, for example, discusses medical identity theft and its profound impact on patients who have been victims, as well as health care systems, both paper and electronic.[3]

I. Overview: Flaws in HHS's approach to privacy and confidentiality issues

We note that the RFI glossed over privacy and failed to mention Fair Information Principles. Privacy and implementation of the full Fair Information Principles will be essential if any new health information technology, including personalized medicine, is to be accepted by the American public. We cannot tell if the apparent lack of positive attention to privacy is a mere oversight or is reflective of an unstated attitude that privacy can be ignored in favor of greater use and sharing of patient data. Either way, the demands of the public for health privacy cannot be ignored or evaded. HHS needs to confront the privacy issue honestly and directly.

Privacy has recently been characterized by HHS as a "barrier to be overcome."[4] This negative focus puts patients and those who care about privacy in a position to have to defend a right that HHS itself should be protecting. The difficulties associated with HHS's current approach to privacy will be heightened in any personalized medicine context, especially given the genetic component of personalized medicine.

Privacy is an integral part of medicine and has been for thousands of years. Privacy must be seen as a positive and integral part of any new system or approach, not as a barrier to be overcome or removed by some clever method or remedy. Unless HHS can make these kinds of adjustments in its approach, it is likely that any project that results from this RFI will be plagued with a lack of public support and other weaknesses that will undermine any potential for long-term success.

Patients rightfully want to retain as much as or more confidentiality, privacy, security, and fair information rights in digitized systems as in paper systems. This also follows for personalized medicine and personalized medicine information systems, including

---

[3] World Privacy Forum <http://www.worldprivacyforum.org>; Medical Identity Theft report, consumer tips, and FAQ: <http://www.worldprivacyforum.org/medicalidentitytheft.html>.

[4] See, for example, the collaboration of 30-plus states in the HISPC (Health Information Security and Privacy Collaboration) project. HHS contracted this privacy and security project to RTI in 2006; the project is set for completion in 2007. The project specifically describes privacy as a barrier to health information exchange in many of its foundational materials. Some of the analyses and activities of the project were conducted with a filter of viewing privacy as a barrier to health information exchange. See < http://www.hhs.gov/news/press/2005pres/20051006a.html>, < http://www.rti.org/page.cfm?objectid=E17E77EA-C0FD-4E32-840FB81A5225AD95>. See also state level materials on this.

electronic health records. HHS must directly address how patients can be given increased rights, access, and privacy through personalized medicine.

HHS can do this by implementing the following:

- ELSI committee
- Chief privacy officer
- Privacy Impact Assessments
- Fair Information Principles

These concepts are discussed in more detail in the comments below.

II. The respected and well-established precedent for a formalized Ethical, Legal and Social Issues (ELSI) committee should be observed by HHS in *all* personalized medicine projects

The World Privacy Forum recommends that HHS establish a formal ELSI committee to oversee all personalized medicine projects, including the planning phases.

ELSI research, planning, and oversight was formalized in 1989 during work on the Human Genome Project. **The U.S. Department of Energy (DOE) and the National Institutes of Health (NIH) devoted 3 percent to 5 percent of their annual Human Genome Project (HGP) budgets toward studying the ethical, legal, and social issues (ELSI) surrounding availability of genetic information**.[5] Any proposed HHS project regarding personalized medicine must do at least this much in terms of dedicated budget and focus regarding ELSI. The World Privacy Forum specifically recommends and requests that a minimum of 5 percent of all budget going toward personalized and genomic medicine be dedicated to ELSI aspects of the projects.

Here is further background on how ELSI came into being, and why it was an integral part of the Human Genome Project:

> The planners of the Human Genome Project (HGP) recognized that the information gained from mapping and sequencing the human genome would have profound implications for individuals, families and society. While this information would have the potential to dramatically improve human health, they also realized that it would raise a number of complex ethical, legal and social issues. How should this new genetic information be interpreted and used? Who should have access to it? How can people be protected from the harm that might result from its improper disclosure or use?
>
> The Ethical, Legal and Social Implications (ELSI) Research Program was

[5] < http://www.ornl.gov/sci/techresources/Human_Genome/elsi/elsi.shtml>.

established to address these issues and has become an integral part of the HGP. ELSI provides a new approach to scientific research by identifying, analyzing and addressing the ethical, legal and social implications of human genetics research at the same time that the basic science is being studied. In this way, problem areas can be identified and solutions developed before scientific information is integrated into health care practice.

The ELSI Research Program is essential to the success of the HGP in the United States and is supported with federal funds. The National Human Genome Research Institute (NHGRI) commits more than $18 million annually from its HGP budget to ELSI research, making it the largest supporter nationwide of research into the ethical, legal and social implications of genetic research. The United States Department of Energy (DOE) Office of Energy Research, which partners with NHGRI in the HGP, also reserves a portion of its funding for ELSI research and education.[6]

A. Justification for formalized ELSI committees in any personalized medicine plan

The ELSI page of the Human Genome Project lists some of the issues that the use of genetic information raises. Personalized medicine raises the same issues, and in some ways makes them more pronounced. For example, genetic information dissemination via electronic health records is a substantial issue that will need to be looked at from multiple and complex angles. There are no simplistic answers or solutions: genomics is a complex area, and the solutions are correspondingly complex. This is not a barrier or an issue to be overcome. It is simply a fact, and should be planned for. An ELSI committee with experience will know how to tackle these issues and provide guidance on implementation.

Here is an overview of the complex issues that personalized medicine will raise, taken largely from the Human Genome Project ELSI materials:

Fairness in the use of genetic information by insurers, employers, courts, schools, adoption agencies, and the military, among others.
- *Who should have access to personal genetic information, and how will it be used?*

Privacy and confidentiality of genetic information.
- *Who owns and controls genetic information?*

Psychological impact and stigmatization due to an individual's genetic differences.
- *How does personal genetic information affect an individual and society's perceptions of that individual?*
- *How does genomic information affect members of minority communities?*

Reproductive issues including adequate informed consent for complex and potentially

[6] <http://www.genome.gov/10001754>.

controversial procedures, use of genetic information in reproductive decision making, and reproductive rights.

- *Do healthcare personnel properly counsel parents about the risks and limitations of genetic technology?*
- *How reliable and useful is fetal genetic testing?*
- *What are the larger societal issues raised by new reproductive technologies?*

Clinical issues including the education of doctors and other health service providers, patients, and the general public in genetic capabilities, scientific limitations, and social risks; and implementation of standards and quality-control measures in testing procedures.

- *How will genetic tests be evaluated and regulated for accuracy, reliability, and utility? (Currently, there is little regulation at the federal level.*)
- *How do we prepare healthcare professionals for the new genetics?*
- *How do we prepare the public to make informed choices?*
- *How do we as a society balance current scientific limitations and social risk with long-term benefits?*

Uncertainties associated with gene tests for susceptibilities and complex conditions (e.g., heart disease) linked to multiple genes and gene-environment interactions.

- *Should testing be performed when no treatment is available?*
- *Should parents have the right to have their minor children tested for adult-onset diseases?*
- *Are genetic tests reliable and interpretable by the medical community?*

Conceptual and philosophical implications regarding human responsibility, free will vs genetic determinism, and concepts of health and disease.

- *Do people's genes make them behave in a particular way?*
- *Can people always control their behavior?*
- *What is considered acceptable diversity?*
- *Where is the line between medical treatment and enhancement?*

Health and environmental issues concerning genetically modified foods (GM) and microbes.

- *Are GM foods and other products safe to humans and the environment?*
- *How will these technologies affect developing nations' dependence on the West?*

Commercialization of products including property rights (patents, copyrights, and trade secrets) and accessibility of data and materials.

- *Who owns genes and other pieces of DNA?*
- *Will patenting DNA sequences limit their accessibility and development into useful products?*[7]

Personalized medicine will raise all of these issues and more. The breadth of the activities

[7] For more discussion on this listing of issues, see <http://www.ornl.gov/sci/techresources/Human_Genome/elsi/elsi.shtml>.

that fall within the scope of the RFI and the potentially sweeping effects on individuals, families, and health care institutions of all stripes are so extensive that the ethical, legal, and social implications need to be addressed. One of our concerns is that the bureaucratic drive toward the high-level goals set out in the RFI and the technical difficulties that will be presented have the potential to overwhelm the conflicts and tradeoffs that will inevitably arise. An ELSI committee is one appropriate way to ensure that these issues will not be lost.

We believe that an ELSI committee must be broad-based, must include qualified members with different perspectives, and must have the ability to speak directly to top management at HHS, to the Congress, and to the American public. An ELSI committee must have the authority to establish its own agenda, control its own staff, and speak in its own voice. **An ELSI committee must be a direct part of the process leading to implementation of the goals identified in the RFI rather than an appendage stuck on for show.**

III. The necessity of a Chief Privacy Officer for personalized medicine projects

In addition to a formalized ELSI committee and ELSI oversight for all personalized medicine proposals and projects undertaken by HHS, the World Privacy Forum recommends that a full time, independent privacy officer be established for this project immediately and that a privacy officer continue in place for the operational life of the project.

This chief privacy officer should be properly qualified and have plentiful and long experience with ELSI, the Privacy Act, Fair Information Principles, HIPAA, and other aspects of health privacy. The chief privacy officer should not have any ties to industry that would influence his or her activities regarding specific projects. The chief privacy officer should be responsible for creating a fair and impartial Privacy Impact Assessment for each proposed or actual project. The chief privacy officer should also be an ex-officio member of the ELSI committee that we have already recommended.

Additionally, the project's privacy officer should:

- Be independent from any institution participating in the project's activities;
- have the ability to report directly to the Congress and to the HHS Secretary;
- not be subject to removal from office without cause;
- be authorized to issue public reports, testify before Congress, hold press conferences, and undertake comparable public activities without the need for clearance from project management;
- have sufficient resources and staff to initiate and conduct audits and investigations of compliance with privacy and security obligations.

IV. The necessity of Privacy Impact Assessments

Each proposed or actual project undertaken by HHS regarding personalized medicine must have a privacy impact assessment (PIA). The PIA must be published prior to any project's implementation, there must be an opportunity for public comments, and HHS must take public comments into account in a meaningful way.

The E-Government Act of 2002 requires federal agencies to prepare a PIA under specified conditions. Whether the Act technically applies to the project and its elements should not determine whether a PIA is completed. The World Privacy Forum recommends that PIAs be required as part of the project and that PIAs be prepared repeatedly during the course of the development of the personalized medicine systems contemplated by the RFI.

Further, the World Privacy Forum recommends that the PIA for the projects exceed the statutory requirements of the E-Government Act. At a minimum, the planners and managers of the projects must be required to consider the PIA and to respond publicly to its findings and recommendations. The PIA could be conducted by the Privacy Officer or by a third party with suitable experience and independence from project planners and likely project participants. The need for independence is crucial. Too often, PIAs are prepared by project managers, contractors, or others with too much of a stake in the project to be objective.

V. The necessity for robust implementation of the full canon of Fair Information Principles for any personalized medicine project

Any personalized medicine project should implement the full canon of Fair Information Principles (FIPs) in a meaningful and complete manner. Fair Information Principles are a set of principles that describe how an information-based society may approach information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security in a rapidly evolving global technology environment. We note that the HIPAA health privacy rule is an express implementation of FIPs. While HIPAA has flaws too numerous to address in these comments, its goal of implementing FIPs in any health information activity is a sound one.

FIPs must be deeply embedded and fully integrated into the projects from the beginning. The World Privacy Forum recommends that each personalized medicine proposal and project be regularly evaluated for appropriate FIPs implementation by ELSI committees and by the chief privacy officer. The implementation of FIPs should be discussed in a privacy impact assessment and again, that PIA needs to be published.

We don't need to remind the Department of its prime role in the original development of FIPs. The first steps toward formally codifying Fair Information Principles began in July 1973, when an advisory committee of the U.S. Department of Health, Education and

Welfare proposed a set of information practices to address a lack of protection under the law at that time. The resulting HEW report, *Records, Computers and the Rights of Citizens: report of the Secretary's Advisory Committee on Automated Personal Data Systems*, set forward key foundational ideas for safeguarding privacy.[8]

In 1980, the Organization for Economic Cooperation and Development (OECD) used these core HEW fair information principles and built upon them to create a set of eight Fair Information Principles codified in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[9] The OECD has historically created internationally-agreed upon codes, practices, decisions, recommendations, and policy instruments. The eight principles OECD published in 1980 were agreed upon by member countries, including the United States, through a consensus and formal ratification process. These OECD guidelines form the basis of many modern international privacy agreements and national laws, and these eight principles from 1980 are referred to by the U.S. Government Accountability Office as key principles for privacy protection.[10]

A. The Eight Fair Information Principles

The principles are as follows:

(From the OECD Guidelines on the Protection of Privacy)

> 1. **Collection Limitation Principle**. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
> 2. **Data Quality Principle**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
> 3. **Purpose Specification Principle**. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
> 4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph [3] except: a) with the consent of the data subject;
> or b) by the authority of law.
> 5. **Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
> 6. **Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use,

---

[8] *Ibid*.
[9] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980). <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.
[10] Koontz, Linda D. *Personal Information: Agencies and Resellers Vary in Providing Privacy Protections*. GAO-06609T at 9 and 10 (April 4, 2006).

as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**. An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

B. Why Fair Information Principles are crucial for personalized medicine

In the decades since the HEW report and the OECD guidelines were published, what has become most clear is that the individuals and organizations who were apprehensive about the loss of fundamental privacy due to lack of protections concomitant with large technological shifts were justified in their concerns. We live in a world that needs unambiguous, even-handed application of the full canon of Fair Information Principles, and this includes the health care sector and any and all activities in the personalized medicine and electronic health record sphere.

The eight principles embodied in the canon of OECD's Fair Information Principles, if applied consistently to personalized medicine projects, would go far in making a positive difference in the privacy protections and data rights afforded to subjects of personalized medicine. In an era of increased digitization of individuals' information, including genomic information, having fundamental fairness of information practices firmly in place is indispensable to a well-balanced, equitable system.

However, the lack of implementation of these principles in personalized medicine projects would go far to engendering mistrust of the projects, and could lead to abuses of the information. Application of only selected pieces of the principles would be equally problematic.

VI. Conclusion

The World Privacy Forum is concerned about a lack of positive responsiveness to privacy issues at DHHS. Recent HHS contracts that have conducted privacy analyses through a filter of viewing privacy as a barrier to be overcome has enhanced the impression that HHS is not necessarily interested in genuinely integrating full-featured privacy protections in its projects.[11] It is crucial that HHS become genuinely and positively responsive to patient and privacy concerns through:

[11] See *supra* note 1.

- A complete and unambiguous implementation of the full range of fair information principles to all programs;
- a full and qualified implementation of one or more ELSIE committees on each project;
- hiring a chief privacy officer for all personalized medicine projects;
- conducting and publishing PIAs regarding all personalized medicine projects.

Additionally, our concerns about medical identity theft, outlined in our report on the topic and in other public comments and testimony before HHS, will be fully applicable to any personalized medicine project.[12] The World Privacy Forum will offer further comments about medical identity theft impacts and effects at a more suitable time, when there are more details about specific personalized medicine projects.

The World Privacy Forum urges HHS to become responsive on the issue of privacy in a positive, proactive way. Privacy is a benefit, not a barrier.

Respectfully submitted,

Pam Dixon
World Privacy Forum

[12] For the report, see *Medical Identity Theft: The Information Crime that Can Kill You*, World Privacy Forum, May 2006, < http://www.worldprivacyforum.org/medicalidentitytheft.html>. The World Privacy Forum has also provided public comments to HHS regarding medical identity theft in testimony before NCVHS (August 2005), testimony before AHIC (September 2006), in comments filed with the President's Identity Theft Task Force – which includes HHS (January 2007), and in comments filed directly with HHS on regulatory reform (September 2005) <http://www.worldprivacyforum.org/comments/medical_privacy_FR05_19788.html> .