WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

On the *Draft Report on Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genetics, Environment, and Disease*

For the Office of the Secretary, Health and Human Services, Secretary's Advisory Committee on Genetics, Health, and Society; the National Institutes of Health; U.S. Public Health Service.

Via email, postal mail, and fax

July 18, 2006

Reed V. Tuckson, M.D., Chair, Secretary's Advisory Committee on Genetics, Health, and Society (SACGHS)
NIH Office of Biotechnology Activities (OBA)
6705 Rockledge Drive
Suite 750
Bethesda MD 20892

Re: Department of Health and Human Services Secretary's Advisory Committee on Genetics, Health, and Society's request for public comment on draft report on "Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genetics, Environment, and Disease." [Federal Register: June 13, 2006. Volume 71, Number 113.]

Pursuant to the notice published in the Federal Register on June 13, 2006 regarding the May 22, 2006 *Draft Report on Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genetics, Environment, and Disease*, the World Privacy Forum respectfully submits the following comments.[1]

The World Privacy Forum is a non-profit, non-partisan public interest research organization.[2] It focuses on in-depth research and analysis of privacy topics, including topics in medical privacy. We have been actively engaged in the area of medical privacy; we testified before The National Committee on Vital and Health Statistics (NCVHS) on the privacy and

[1] Department of Health and Human Services Secretary's Advisory Committee on Genetics, Health, and Society request for public comment on draft report on "Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genetics, Environment, and Disease." 71 Fed. Reg. 34,146 (June 13, 2006).
[2] <http://www.worldprivacyforum.org>.

confidentiality of electronic health records and the proposed National Health Information Network, and recently, we published the first major report on medical identity theft.

The May 22, 2006 draft report on *Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genetics, Environment, and Disease*[3] states in its opening paragraphs:

> Large longitudinal population studies, involving the collection of data about and biological specimens from hundreds of thousands of people, offer one promising approach to learning more about the relationships among genes, the environment, and common disease. The creation of such a large database and biobank could serve as an essential research resource for hundreds, if not thousands, of research studies. For many, such a large-scale project is a logical next step following the complete sequencing of the human genome. In the United States, the National Institutes of Health (NIH) is investigating the possibility of mounting a large population cohort project.[4]

The draft report also notes that "the nature of the information that will be derived from it raises ethical, legal, social and public policy concerns that could be unique and/or significant, particularly in view of the number of potential participants." The World Privacy Forum agrees that substantial policy issues are raised by the prospect of a U.S. large population cohort project for the study of genetic variation and disease, and appreciates the opportunity to comment on the draft report.

The draft report appropriately raises a large number of complex scientific and policy questions associated with a large U.S. population cohort project on genes and diseases. Our comments are confined to those issues relating to privacy and policy matters associated with privacy. Specifically, our comments address the following issues: the structure of the project and the law, the need for a privacy officer, the necessity of a privacy impact assessment (PIA), third party use of project records, subject identifiability, the proposed working group, and issues relating to HIPAA.

I. Project Structure and the Law

The draft report does not describe in any detail the organization of the research project or the relationship between the many entities that will be involved in it. This non-specific approach may be understandable at this stage, but it seems apparent that the project will necessarily involve institutions that have different roles, legal requirements, and privacy regimes.

For example, some health care providers will be suppliers of patient information. Some providers will be suppliers of patient information and researchers with respect to information about their own patients. Some entities that are health care providers in one context will only be

---

[3] Referred to as "draft report" hereafter.

[4] *Policy Issues Associated with Undertaking a Large U.S. Population Cohort Project on Genes, Environment, and Disease*. Public Comment Draft, May 22, 2006, around lines 41 to 47. <http://www4.od.nih.gov/oba/SACGHS/public_comments.htm>.

researchers with respect to the project. Some researchers will not be health care providers at all. Some who supply information may be neither health care providers nor researchers.

Different entities will be subject to different privacy laws. Most health care providers involved in the project will be subject to HIPAA. Some other suppliers of research subject information (e.g., insurers) will also be subject to HIPAA. Some suppliers of research subject information may not be covered entities at all. Researchers, for example, may not be covered entities, and they will not be subject to HIPAA.

The National Institutes of Health (NIH) may be unique in that it is not subject to HIPAA. It may be the only health care provider of any size not subject to HIPAA. The NIH is, however, subject to the Privacy Act of 1974. Other federal agencies likely to be participants in the project will be subject to both HIPAA and the Privacy Act of 1974. Every health care provider and researcher will be subject to applicable state health privacy laws, except for federal agencies that are generally not covered by state laws. Requirements of the Clinical Laboratory Improvement Amendments may add further layers of complexity, with the effect varying from state to state and from lab (CLIA lab) to lab (non-CLIA lab). The draft already discusses some of the issues of overlapping laws, but a much more intensive review will be required.

Some research subject information essential for the project will likely come from foreign sources. Many other nations have omnibus privacy laws that often include strict rules for the export of personally identifiable information to third countries. When it is lawful to export personally identifiable information to the United States, that information sometimes comes with additional privacy protection requirements that will exceed U.S. standards.

Some obvious consequences of all of these differing and overlapping requirements are:

1. The privacy rights of a research subject may vary depending on which institution holds the subject's information and, possibly, where that institution is located. The privacy rights may also vary from data element to data element within a record maintained by a health care provider or by a researcher.

2. The responsibilities of health care providers and researchers will vary depending on their particular role with respect to research subject information and, possibly, where they are located.

3. Research subject information will necessarily flow from one privacy regime to another privacy regime. That may result in either the enhancement or degradation of privacy rights. In some cases, both may occur at the same time.

4. Research subject information will flow from one regime where there is privacy protection to another where privacy protection is entirely or mostly absent. For example, a researcher is typically not to be subject to any privacy statute or law (other than the minimal standards suggested in the Common Rule).

None of the individual circumstances described here are unique to this project. Indeed, it is likely the case that all of these circumstances are already present in some existing research projects. What distinguishes the project at hand from others are:

1. The large scope of this project;
2. the perceived sensitivity of the information;
3. the likely visibility of the project; and, most importantly,
4. the willingness of planners to address privacy matters at this early planning stage.

The structural and legal problems accompanying this project appear to be, and in fact are, so challenging because no one has sought to address them before. For many research activities involving health information, neither the researchers nor Institutional Review Boards pay much attention to privacy. No law establishes fair information practices for researchers (with the exception of the Privacy Act of 1974 with respect to federal agency researchers). There are no "industry" standards for research privacy. There is no formbook of research privacy policies from which a researcher can copy a policy for his or her project.

None of these comments is intended to suggest a general absence of concern about privacy on the part of the research community. As with health providers in the pre-HIPAA era, researchers pay lip service to privacy, even if many are in reality are actually doing little about it. Laws pertaining to research records generally address how researchers can obtain records that they need. Some laws, for example, provide limited protection for research records against compelled disclosure.[5] However, most elements of fair information practices remain unaddressed in the research world.

A. Potential ways to address privacy issues raised by the project

We see three ways to address privacy matters in this project.

First, a law establishing privacy standards for health researchers could be proposed. This would admittedly be a difficult undertaking with highly uncertain prospects for success and with a scope that far exceeds the requirements of the project. Nevertheless, the privacy problems identified here are inherent in most health research and in much other social science research.

Second, a law establishing privacy standards for this particular project could be proposed. The substantive and political difficulties would be somewhat less challenging for a law aimed at one specific health research project rather than all health research projects, but the prospects for success would remain just as uncertain. However, some of the other public policy dilemmas raised in the request for comments might benefit from legislative resolution, not to mention legislative support and funding.

Third, a privacy policy for the project could be developed and made a requirement for all participants. Given the differences in application of currents laws to information and institutions, this approach would be challenging but certainly not impossible. A floor of privacy

[5] See e.g., 42 U.S.C. 241(d)

protections established as a condition of participation by researchers can afford data subjects sufficient rights without creating too many legal or practical complexities. Privacy laws generally permit higher standards to be applied so that a reasonable privacy policy will not create actual conflicts in most instances. In some instances, additional protections may be needed for AIDS, psychiatric, substance abuse, genetic, and other narrower classes of data.

One advantage inherent to the development of a formal privacy policy is the opportunity to ask the European Union to recognize that the privacy policy meets standards of adequacy that support the export of information from EU Member States to the United States.[6] A finding of adequacy would simplify international transfers enormously, and it would be a useful precedent for other research activities. However, obtaining a finding for what would essentially be an industry code is not likely to be accomplished easily or quickly. It is, however, something that would be a useful model for other health research projects conducted in the United States with international participation.

The project's privacy policy should be based expressly on Fair Information Practices (FIPs). FIPs are a set of principles for addressing concerns about information privacy. FIPs are especially significant because they form the basis of many privacy laws in the United States and, to a much greater extent, around the world.[7] FIPs offer a framework for privacy policy, policy discussions, and legislation. FIPs do not, however, automatically translate into a privacy policy for any given set of data or activity. Establishing a specifically applied policy requires the balancing of competing values, cost considerations, and practicality. It is worth noting that the HIPAA health privacy rules are "are based on common principles of fair information practices."[8]

Much more can be said about how FIPs could and should apply to the project. However, that discussion seems premature at present, and we will reserve further comments until a later time.

The three paths that we suggest are not mutually exclusive. Each of the approaches would take considerable effort. The third is the one most within the control of those who would advance the project toward implementation.

The World Privacy Forum recommends that, at a minimum, the project develop a comprehensive privacy policy that all researchers and clinicians participating in the project must strictly adhere to. That policy must include a mechanism that holds participants accountable for compliance with the privacy policy.

---

[6] Council Directive 95/46, art. 25.2, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L281/47), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[7] The most commonly cited version of FIPs is from the Organization for Economic Co-operation and Development. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[8] Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82461, 82487 (Dec. 28, 2000).

II. Necessity of a Full-Time Privacy Officer

A project of the proposed size and duration should have a full-time privacy officer with functions limited to the project. The project's privacy officer should:

- Be independent from any of the institutions participating in the project's research activities;
- report directly to a board of directors or comparable governing organization for the project;
- 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;
- have the authority to accept and act upon complaints from research subject, project participants, and members of the public;
- be authorized to recommend that a project participant be removed from the project or sanctioned in other ways;
- be empowered to propose changes in the privacy policy.

The World Privacy Forum recommends that a full time, independent privacy officer be established for the project at an early stage in project planning and that a privacy officer continue in place for the operational life of the project.

III. The Need for a Privacy Impact Assessment

The project also needs a detailed and thorough privacy impact assessment (PIA). This PIA needs to be made publicly available well in advance of the inception of any project.

The E-Government Act of 2002[9] requires federal agencies to prepare a PIA under specified conditions. The law may not apply to a project likely to be funded by a grant, but it is possible that the statutory PIA obligation will attach. Regardless, the World Privacy Forum recommends that a formal and complete PIA be undertaken at an early stage in project planning. Further, the World Privacy Forum recommends that the PIA for the project exceed the statutory requirements of the E-Government Act.

At a minimum, the planners and managers of the project 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 PIA must be published publicly, as research subjects have a strong and defensible interest in seeing this information.

[9] 44 USC 3501 note.

IV. Third Party Use of Project Records

The files and databases created for use in the project have the potential to attract a bevy of interested users who have no relationship to the project. Users could include law enforcement, national security agencies, private litigators, welfare agencies, and others. Existing laws establishing protection against compelled disclosure may be of assistance in protecting records from third parties.

The *certificate of confidentiality* laws available within the Department of Health and Human Services include 42 U.S.C. § 299c-3(c), 42 U.S.C. § 242m(d), and 42 U.S.C. § 241. These laws offer covered records some disclosure protection, but they have limits that must be explored and recognized. The mixing of research and clinical records that may occur as part of the project could have the effect of further weakening the already limited protections of certificates. Further, most certificates protect against compulsory disclosures and do not expressly prohibit consensual disclosures.

The need for better statutory protection for research records is an argument for seeking legislative authorization for the project.

The World Privacy Forum recommends that the project planning assess the scope and gaps of existing certificate of confidentiality laws. Only after that assessment has been conducted and completed will it be possible to determine if statutory protections are adequate, whether additional statutory protection is required, and what data subjects who voluntarily participate in the project must be told about the legal risks of participation.

Despite any shortcomings in the certificate of confidentiality laws, the World Privacy Forum recommends that steps be taken so that the project has the benefit of the protections available in one or more of these laws.

V. Identifiability

The draft recognizes that identifiability will be an important issue in the project. The draft includes (around line 1590) a reasonable discussion about the prospect that the DNA sequence data may become identifiable. The World Privacy Forum observes that it appears to be inevitable that DNA sequence data will be identifiable at some point in the future because of the rapid development of DNA databases for law enforcement, medical, and other purposes.

This is only one type of identifiability problem that the project will encounter. As the work of Professor Latanya Sweeney has demonstrated, the de-identification of health records is increasingly difficult to accomplish.[10] The project must address identifiability issues for all research subject information that will be shared.

---

[10] See, e.g. Malin, B. and Sweeney, L. Determining the Identifiability of DNA Database Entries. *Proceedings, Journal of the American Medical Informatics Association*. Washington, DC: Hanley & Belfus, Inc. Nov 2000; 537-541. See also <http://lab.privacy.cs.cmu.edu/people/sweeney/> and Carneige Mellon Data Privacy Lab: Genomic Privacy Project <http://privacy.cs.cmu.edu/dataprivacy/projects/genetic/index.html>.

Legal standards for identifiability are generally unsophisticated, incomplete, and inconsistent. The HIPAA approach to de-identified data is better than most, but it does not solve all of the problems likely to arise. The World Privacy Forum recommends that the project develop its own high standards for de-identification based on appropriate legal, policy, and technical measures. Identifiability is an issue that the project's PIA and published privacy policy should address.[11]

VI. Working Group

The draft includes a recommendation (around line 309) that the Director of NIH convene a working group to develop a set of recommended best practices and standard operating procedures for the project. The World Privacy Forum supports this recommendation.

However, the working group should have adequate and preferably robust representation from the civil rights, patient advocacy, and privacy communities. The World Privacy Forum also recommends that public input on policies and procedures be mandatory.

VII. HIPAA

The discussion of HIPAA in the draft includes this observation (around line 1615): "In most cases, the Privacy Rule will require authorization from individuals (subjects) to use their protected health information in research, unless an exception applies." That statement is true, but since there is always an exception available for research (with only IRB or privacy board approval as a prerequisite), the statement is a bit disingenuous.

As a practical matter, patient authorization is rarely required for records-based research. The role of patient authorization for the project is, as the draft already states, something that requires more attention.

The World Privacy Forum cautions against casual characterization of the HIPAA privacy rule as providing a high level of protection for privacy. The rule has its value, but it is filled with compromise, weak standards, and insufficient procedures. Data subjects who participate in the project face significant additional legal and other risks to their privacy because of the breadth of data to be collected, the long-term life of the study, and the potentially sensitive classes of data that will be used.

These factors, together with the shortcomings of HIPAA and the lack of any formal privacy requirements for most research records places patients at some significant additional jeopardy. Simply meeting the weak HIPAA privacy requirements is not likely to be sufficient to protect data subjects.

---

[11] Certain aspects of identifiability will also be at issue in regards to any data breaches that occur. While our comments have not focused on data and computer security, the prospect of data breaches of the project information is a genuine risk, and should be considered in relationship to identifiability issues and computer security issues. See <http://www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html>, I (D) "Security Breaches."

VIII. Conclusion

The World Privacy Forum appreciates the opportunity to submit comments to SACGHS regarding the draft report. We hope that the NIH will obtain input from and increase the participation of privacy, civil liberties, and patient advocacy groups regarding the complex, important, and challenging issues a large cohort project raises.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
+1 760.436.2489