WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

On the Draft Report of the Secretary's Advisory Committee on Genetics, Health, and Society, *Realizing the Promise of Pharmacogenomics: Opportunities and Challenges*

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 e-mail and fax

May 23, 2007

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

Dear Dr. Tuckson:

The World Privacy Forum welcomes the opportunity to comment on the draft report of the Secretary's Advisory Committee on Genetics, Health, and Society titled *Realizing the Promise of Pharmacogenomics: Opportunities and Challenges* published in March 2007. This is a response to the request for comments that appeared in the Federal Register on March 28, 2007, 72 Fed. Reg 14577.

Introduction

The World Privacy Forum is a non-profit, non-partisan public interest research organization. It focuses on in-depth research and analysis of privacy topics, including topics in medical privacy, financial privacy, and other aspects of privacy.[1]

These comments focus on the privacy implications of the draft report. We want to state our basic view as clearly and as simply as we can. Privacy is not a barrier to any aspect of the practice of medicine. It is an inherent part of medical care and has been since the dawn of medicine. Privacy is not something to be evaded, avoided, undermined, dismissed, or overcome. The need for privacy must be accepted and incorporated in any medical setting, including research.

The World Privacy Forum recognizes the value of patient data for research, and we express no fundamental objection. However, the terms of any data use or data sharing for research are

[1] <http://www.worldprivacyforum.org>

important, the effects on privacy must be evaluated, and the fundamental goals of privacy must be incorporated. As with any other secondary use of health treatment records, the sharing of patient data for research affects the privacy interests of patients. That is true regardless of the scope or importance of the research. Data sharing can be justified notwithstanding its negative privacy consequences, but there must be a suitable recognition and accommodation of patient privacy interests.

So we are a bit put off by this recommendation on page 8 of the report:

> HHS should work with the private sector to identify obstacles to data sharing and to develop solutions to overcome these obstacles (e.g., legal and data confidentiality assurances, intellectual property protections).

Our objection is as much to the language as to the policy. We are unhappy that the Department of Health and Human Services in many of its activities already tends to view privacy as a *barrier* to its plans for greater exploitation of patient information for treatment and other purposes. We would much prefer to see an acknowledgement of the inherent necessity of privacy in the health care system that extends beyond lip service. If patients walk away from research activities or from treatment because they do not think that their privacy interests are adequately protected, nothing will be accomplished. Accommodating privacy has costs and consequences that cannot be entirely *overcome*. We readily acknowledge that privacy must compete with other basic health care objectives, but we object when those seeking to attain those other objectives are readily prepared to jettison privacy entirely in pursuit of those other goals.

Our general conclusions about privacy and medicine are true for pharmacogenomics (PGx) just as for any other aspect of medicine. We do not argue here that genetic information inherently requires extra protection beyond that afforded to other health information. We suggest that genetic information, like some other health information, has some characteristics that may call at times for different application of standard privacy policies. For example, conflicts between the interests of related individuals may be more intense with genetics than with most other classes of health information.

We observe that existing protections for all health information have significant inadequacies. We do not expect the SACGHS to fix those problems, but we caution against any assumption that current medical privacy law and policy suitably resolves all health privacy concerns. The HIPAA health privacy rule has many shortcomings, and the existing problems will only grow worse as uses of patient information are expanded through networks and otherwise.

We also caution about too much reliance on HHS to protect privacy interests. The Department has too many other roles in the health care system to be trusted to always strike a fair balance when privacy matters are at stake. Other stakeholders need to be involved when choices are to be made, privacy impact assessments are needed, and balancing of interests is required.

Finally, we reaffirm the importance of Fair Information Principles (FIPs) in establishing policies for the use of any personal information. Fair Information Principles are an internationally accepted 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 any PGx projects and data flows from the beginning.

The Department played a 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.[2]

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.[3] 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.[4]

Marketing

We begin our main comments with marketing issues because there is not enough awareness in the health policy world about existing trafficking in health care information. We are encouraged by the Committee's attention (page 79) to the marketing opportunities that may arise if PGx tests evolve into consumer products. We think that there are additional related concerns.

The interest of marketers in personal health information is strong. We suggest that you look up the web site of Direct Magazine at <http://listfinder.directmag.com/market> and enter the keyword *ailments* into the "list finder" search box. You will find page after page of mailing lists that offer the names and addresses of individuals by ailment, including diabetes, Crohn's disease, Lupus, heart disease, asthma, and many others. Purveyors of mailing lists and personal profiles would be happy to add genetic characteristics to their files.

---

[2] <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

[3] Organisation for Economic Co-operation and Development. *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>.

[4] General Accounting Office, *Agency and Reseller Adherence to Key Privacy Principles* 1-2 (April 4, 2006) (GAO-06-421).

We expect that one consequence of the availability of additional genetic information about individuals will be an increase in personally directed advertising hawking expensive prescription medication, new testing methods, and useless treatments. We leave it as an exercise for the Committee to speculate how purveyors of fraudulent weight loss remedies might use new genetic findings and genetic information to sell their wares.

These detrimental activities do not outweigh the development of beneficial uses of PGx. However, they do suggest the need for stronger controls over patient information, restrictions on direct-to-consumer (DTC) advertising, and better enforcement of consumer protections.

Research vs. Treatment

The draft report focuses much, but not all, of its attention on research activities. We want to underscore the major differences for privacy between research and treatment activities. Under current health privacy policies, health information in the hands of those who are not HIPAA covered entities is not subject to HIPAA privacy protections. Thus, records subject to HIPAA in the hands of a treating physician are not necessarily subject to HIPAA when disclosed to a researcher. A registry or other database of health information maintained for research purposes is not likely to be covered by the HIPAA privacy rules.

Under the right circumstances, research records can have significant protections against secondary use through certificates of confidentiality. In general, certificates of confidentiality authorize researchers to resist compulsory legal demands (e.g., subpoenas and court orders) for identifiable research information about individuals. By providing a defense against compelled disclosure, certificates provide a defense against legal obligations to disclose records to law enforcement agencies, private litigants, and others who may have an interest in the records for purposes unrelated to the purpose for which the records were compiled. One statute that establishes a certificate program is 42 U.S.C. § 241.[5]

By contrast, when health research records are maintained by federal agencies and are not protected by certificates, the records can be subject to secondary uses, including for law enforcement purposes. Treatment records covered by HIPAA privacy rules may also be disclosed for numerous secondary purposes without patient consent and without court orders. For example, HIPAA records can be disclosed for law enforcement purposes in response to oral requests with minimal threshold requirements and for national security purposes with no threshold requirements at all.

Patient records held by researchers who are not federal agencies are also at greater risk for secondary use when not covered by certificates of confidentiality. While institutional review boards (IRBs) may impose some conditions on reuse or redisclosure of patient records by researchers, we doubt that all IRBs are knowledgeable enough to impose an adequate set of

[5] Other statutes that provide for certificates of confidentiality or the equivalent include: 42 U.S.C. § 242m(d); 42 U.S.C. § 299c-3(c); 42 U.S.C. § 290aa(n); 42 U.S.C. § 3789g(a); 42 U.S.C. § 10604(d); and 44 U.S.C. § 3501 note. See the NIH's Certificates of Confidentiality Kiosk at <http://grants.nih.gov/grants/policy/coc/index.htm>. We do not mean to suggest that existing certificate of confidentiality laws are perfect, but they offer a type of protection not otherwise available for health research records.

rules. We have even more doubts about the ability of IRBs to oversee the enforcement any restrictions that they may impose.

We recommend that all research activities that involve any type of identifiable health information be required to have certificates of confidentiality. We also recommend that all research activities that involve any type of patient-specific genetic information be required to have certificates of confidentiality, whether that information appears identifiable or not. The World Privacy Forum believes that the capability of identifying individuals from subsets of genetic information will expand greatly in the future. Portions of an individual's genetic code that appear to be non-identifiable today may become identifiable tomorrow as a result of new technologies or other data repositories maintained by other researchers or even by law enforcement agencies.

The report needs to pay considerably more attention to the transition from research activities to routine treatment applications of PGx technology. When genetic sequencing becomes a standard treatment activity, the sequences can be readily available to law enforcement under current HIPAA privacy rules. With the looming possibility of a national health network, it is fully conceivable that law enforcement professionals could have virtually unlimited access to patient records through, for example, the ease of a network terminal.

When DNA sequence information becomes a routine part of a health record, that information may leak out of the health care system and end up in the files of employers, insurers, pharmaceutical manufacturers, purveyors of personal health record services, marketers, and others. There is nothing unique here about sequence information. Considerable amounts of patient information leak out of the health care system today.

The jump from research to treatment has enormous implications for privacy, and the non-medical use of genetic sequence information may have negative consequences for individuals. The Committee should not focus too narrowly on the medical applications of PGx technology and ignore the other consequences. We can envision the possibility that routine integration of PGx into medical practice will result in greatly expanded DNA analyses for patients, including the possibility of full sequencing for all newborns. That could result in a DNA database akin to – or even more comprehensive than – the existing FBI fingerprint database. We envision the need for stronger privacy rules and laws, and the Committee should consider what type of additional protections might be needed.

Identifiability

The draft report considers the use of coding or encryption to protect privacy of patients. We support better technical measures to mask identity. Coding identifiable information, if done properly, offers some protection for privacy. However, information that does not have any overt identifiers may nevertheless be capable of reidentification. The work of Carnegie Mellon Professor Latanya Sweeney offers overwhelming evidence on this point. We refer you in particular to B. Malin and L. Sweeney, *How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity*

Protection Systems.[6] We quote the paper's abstract here because it makes the point that removal or encryption of explicitly identifiable genetic information is not sufficient.

> The increasing integration of patient-specific genomic data into clinical practice and research raises serious privacy concerns. Various systems have been proposed that protect privacy by removing or encrypting explicitly identifying information, such as name or social security number, into pseudonyms. Though these systems claim to protect identity from being disclosed, they lack formal proofs. In this paper, we study the erosion of privacy when genomic data, either pseudonymous or data believed to be anonymous, is released into a distributed healthcare environment. Several algorithms are introduced, collectively called REIdentification of Data In Trails (REIDIT), which link genomic data to named individuals in publicly available records by leveraging unique features in patient location visit patterns. Algorithmic proofs of re-identification are developed and we demonstrate, with experiments on real-world data, that susceptibility to reidentification is neither trivial nor the result of bizarre isolated occurrences. We propose that such techniques can be applied as system tests of privacy protection capabilities.

The enormous amount of personal information available from public and private sources means that the realm of truly non-identifiable personal information is shrinking every day. You should not assume that genetic information will be exempt from this trend. We fully expect that patient genetic information will eventually end up in the possession of commercial data brokers and other private actors who may not be subject to privacy rules. We do not believe that the Committee should casually assume that coding or encryption will provide a broad or permanent solution to privacy concerns.

We are more positive about the use of what the draft report calls *controlled data-release arrangements, where parties must commit to protecting privacy and confidentiality before being granted access* (page 43). Data use agreements of the type described in the HIPAA health privacy rule have a place and can provide a layer of protection. We recommend that data use agreements expressly provide that data subjects are intended third-party beneficiaries of the legal, technical, and administrative protections established by the agreements. Otherwise, data subjects may have rights without remedies, and the intended protections may have little meaning.

Even the most carefully drafted and complete data use agreement has its limits. A data use agreement can have utility in research, public health, and health oversight activities where the need for identifiers is often narrow and the volume of data is typically large. However, data use agreements are not likely to have any applicability in a treatment context where the identity of the patient is always known and where the use of overt identifiers is often essential. Privacy responses that work for research do not necessarily solve treatment problems, and vice versa.

<u>Privacy Solutions</u>

[6] 37 Journal of Biomedical Informatics 179-192 (2004), <http://privacy.cs.cmu.edu/dataprivacy/projects/trails/dnaTrails.html>.

We note the recommendation (page 11) for more funding of research on the ethical, legal, and social implications of PGx. We agree, but we think that this is an inadequate response. ELSI research is welcome, but ELSI research in the past has tended to sit on a shelf or in a journal, completely divorced from the policy process. If ELSI activities on PGx result in more of the same, then they may be pointless.

What is needed is a method for assuring that ELSI issues – especially including privacy – are addressed when decisions are made about funding research, approving protocols, establishing databases, and implementing the results of research in treatment activities. Two types of institutions exist for these purposes.[7]

First, the World Privacy Forum recommends that a full time, independent privacy officer position be created for PGx activities. This privacy officer should be properly qualified and have plentiful and long experience with ELSI, the Privacy Act, Fair Information Practices, HIPAA, and other aspects of health privacy. In addition, the privacy officer should be responsible for creating a fair and impartial Privacy Impact Assessment for each proposed or actual major project.

Additionally, the project's privacy officer should:

- be independent from any institution participating in the project's activities;
- serve as an ex-officio member of any PGx ELSI committee;
- 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.

Because PGx privacy matters will include research, treatment, policy, and other issues, we suggest that the privacy officer should be in the Office of the Secretary. It would be ideal if the position of HHS privacy advocate were reestablished and provided with sufficient resources to carry out a broader mission, including PGx privacy.

Second, privacy impact assessments (PIAs) should be required for significant PGx activities funded by the federal government. Each PIA should be published for public comment, and the comments should be considered by decision makers. The E-Government Act of 2002 requires federal agencies to prepare a PIA under specified conditions. Whether or how the Act may apply to PGx activities should not determine whether a PIA is completed. We recommend that PIAs be required for significant federal PGx activities, including major research databases and policy decisions for PGx. We do not envision that each PGx research protocol will need its own PIA, however.

[7] We are intentionally ignoring IRBs here because we do not believe that IRBs generally have the skills or capability of addressing privacy.

We also recommend that the PIA exceed the statutory requirements of the E-Government Act. At a minimum, decision makers 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.

Conclusion

Thank you for the opportunity to comment on the Committee's draft report on pharmacogenomics. We have no doubt that it is possible to incorporate new advances in medicine without unduly impinging on the privacy that patients appropriately demand from the health care system. We hope that our suggestions will be helpful in making progress with pharmacogenomics in combination with robust privacy protections.

Respectfully submitted,

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