

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE PRESIDENTIAL COMMISSION FOR THE STUDY OF BIOETHICAL ISSUES

of the

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Comments on Issues of Privacy Access With Regard to Human Genome Sequence Data

May 25, 2012

By notice published on March 27, 2012, the Presidential Commission for the Study of Bioethical Issues (the “Commission”) of the Department of Health and Human Services (“HHS”) has invited comment on issues of privacy and access with regard to human genome sequence data.¹ The Commission is interested in “policies, practices, research, and perspectives on issues of privacy and data access as they relate to the integrations of large-scale human genome sequencing into research and clinical care.”² Specifically, the Commission would like public comments applicable to, *inter alia*, issues related to “the privacy of individuals, research subjects, patients and their families; models and mechanisms for protecting privacy, in both genetic/genomic databases and biobanks, but also in large databases of sensitive information; balancing individual and societal interests with regard to the sharing of and access to large-scale human genomic

¹ Request for Comments on Issues of Privacy and Access With Regard to Human Genome Sequence Data, 77 Fed. Reg. 18247 (proposed Mar. 27, 2012).

² *Id.*

data; who should have access to these data and who should control access; and the access to genetic/genomic information by law enforcement entities.”³

The Electronic Privacy Information Center (“EPIC”) submits these comments to recommend models and mechanisms for protecting privacy as the government moves closer to sequencing human genomes. EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has been a longtime advocate for genetic privacy and medical record privacy.⁴ Genetic information that is uniquely linked to identifiable individuals raises distinct privacy concerns. Unlike other forms of personally identifiable information, genetic data and corresponding biometric information are truly unique identifiers.⁵ They are unlike names and dates of birth, which can be shared by millions of people. They are unlike residential addresses and places of employment, which are easily found over the Internet. They are even unlike social security numbers in that individuals are not required to provide their genetic data for tax purposes, loan applications, or government benefits. All of these distinctions currently limit unauthorized access, disclosure, and other abuse of

³ *Id.* at 18247-48.

⁴ See, e.g., EPIC: Genetic Privacy, <http://epic.org/privacy/genetic/>; EPIC: Medical Record Privacy; Br. *Amicus Curiae* Electronic Privacy Information Center (EPIC) *et al.*, Supp. Pet. *Herring v. United States*, 555 U.S. 135 (2009), available at http://epic.org/privacy/herring/07-513tsac_epic.pdf; Br. *Amicus Curiae* Electronic Privacy Information Center (EPIC) Supp. Apl., *U.S. v. Pool*, 621 F.3d 1213 (9th Cir. 2010), available at http://epic.org/amicus/pool/EPIC_brief_Pool_Final.pdf; Br. *Amicus Curiae* Electronic Privacy Information Center (EPIC) Supp. Apl., *U.S. v. Kinkade*, 379 F.3d 813 (9th Cir. 2004), available at http://epic.org/privacy/genetic/kinkade_amicus.pdf; Br. *Amicus Curiae* Electronic Privacy Information Center (EPIC) Supp. Apl., *Maryland v. Raines*, 857 A.2d 19 (Md. 2004), available at http://epic.org/privacy/genetic/raines_amicus.pdf;

⁵ Biometrics.gov, Biometrics Frequently Asked Questions, available at <http://biometrics.gov/Documents/FAQ.pdf>.

genetic data and biometrics. But this is likely to change. As the government increases its collection of genetic/genomic data, EPIC believes that it is imperative that privacy laws and policy concerning health data are strictly enforced.

I. GINA and the HIPAA Privacy Rule are Two Privacy Laws That Provide Guidance for Protecting Genetic Data Privacy

EPIC acknowledges the fact that “science is at a point where relatively inexpensive, rapid sequencing of whole human genomes appears not only likely, but imminent,”⁶ and that human genome sequencing can be beneficial to the healthcare field. EPIC also agrees with Professor Anita L. Allen, Commissioner for Presidential Commission for the Study of Bioethical Issues, in that “privacy still matters.”⁷ In her 2007 paper *Face to Face with “It”: And Other Neglected Contexts of Health Privacy*, Commissioner Allen explores the competing interests of health disclosure and personal privacy. Allen writes

The new openness about health concerns has public health and private health benefits. For example . . . [f]reely sharing health information with nurses and doctors makes it possible to receive appropriate medical care. . . The same is true of sharing health information with government administrators who process applications, for example, Medicaid, or who administer public health services.⁸

Notwithstanding that health data disclosure can be beneficial, Allen notes that people [still] rely upon privacy to help control or limit health disclosures that could result in tangible, material losses. Potential losses can be major. They include loss of employment, loss of insurance, loss of school choice, loss of community standing, and loss of intimacy. Protecting health information through privacy policies serves and important material loss

⁶ 77 Fed. Reg. 18247.

⁷ Anita L. Allen, *Face to Face with “It”: And Other Neglected Contexts of Health Privacy*, 151 PROCEEDINGS OF THE AMERICAN PHILOSOPHICAL SOCIETY 300, 301 (2007).

⁸ *Id.*

minimization function in a world in which discrimination and rejection can flow from news of health or genetic status.⁹

Because of these types of material losses due to medical data disclosure, Commissioner Allen states, “[i]n our liberal society we need the legal policies we have got; policies that presumptively vest certain alienable rights to control health data disclosures in the individual.”¹⁰

The Genetic Information Nondiscrimination Act (“GINA”) is one example of a legal policy that vests certain rights to control health data access as the government facilitates human genome sequencing. GINA prohibits employers and health insurance issuers from discriminating based upon genetic information.¹¹ GINA implicates privacy and health data disclosures because the law proscribes employers and health insurance issuers from requesting, requiring, or purchasing individuals’ genetic information.¹² The law also protects employee family members and dependents from nonconsensual genetic data disclosure.¹³ GINA creates a private right of action for employees that allege employment discrimination based upon their genetic information.¹⁴ Moreover, for the circumstances under which employees or individuals covered by insurance plans do disclose genetic information (for research purposes, or for health wellness programs, for example) GINA mandates that employers and health insurance issuers protect the confidentiality of the information.¹⁵

⁹ *Id.* at 307.

¹⁰ *Id.* at 308.

¹¹ Genetic Information Nondiscrimination Act of 2008, PL 110–233, May 21, 2008, 122 Stat 881.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

GINA is an instructive model for protecting genetic privacy, and EPIC recommends that the Commission consider the law as a starting point to protect genomic data. GINA can, however, be improved, because it does not currently create property rights in individual DNA,¹⁶ allowing others in possession of DNA to monetize and commodify the data uniquely linked to another individual. EPIC therefore recommends that the Commission address individual DNA ownership rights of genomic data sequencing, and give individuals greater control over their genetic data.

The Health Insurance Portability and Accountability Act (“HIPAA”) Privacy Rule (45 CFR Parts 160 and Subparts A and E of Part 164) is another law that can guide the Commission on genetic privacy policy. The Privacy Rule establishes a federal mandate for individual rights in health information, imposes restrictions on uses and disclosures of protected health information (“PHI”), and provides for civil and criminal penalties for violations. PHI includes individually identifiable health information related to the past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.¹⁷ Even the fact that an individual received medical care is protected information under the regulation.¹⁸

The individual, who is the subject of Protected Health Information (PHI), has the following rights under the Privacy Rule:

- Right to access, inspect and copy PHI held by hospitals, clinics, health plans and other "covered entities," with some exceptions

¹⁶ See also Anita L. Allen, *Privacy Law and Society* 761 (2d ed. West 2011).

¹⁷ Department of Health and Human Services Definitions, 45 C.F.R. § 160.103 (2007).

¹⁸ *Id.*

- Right to request amendments to PHI held by "covered entities"
- Right to request an accounting of disclosures that have been made without authorization to anyone other than the individual for purposes other than treatment, payment and health care operations
- Right to receive a Notice of Privacy Practices from doctors, hospitals, health plans and others in the health care system
- Right to request confidential communications of PHI, e.g., having PHI transmitted to a different address or a different telephone number
- Right to request restrictions on uses or disclosures, although the "covered entity" receiving the request is not obligated to accept it
- Right to complain about privacy practices to the "covered entity" and to the Secretary of Health and Human Services ¹⁹

The HIPAA Privacy Rule applies to genetic information that is “individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse.”²⁰

Although the HIPAA Privacy Rule can provide a blueprint for protecting genetic data privacy, privacy experts agree that the Rule “does not protect privacy as well as it should.”²¹ To this end, in 2009, the Institute of Medicine (“IOM”) of the National Academies released a report on privacy and medical research, recommending guidelines for stronger privacy protection and transparency in medical research and data collection. Some of IOM’s recommendations for federal agencies are detailed below:

- Clarify the circumstances under which DNA samples are considered

¹⁹ Department of Health and Human Services Privacy Act Regulations, 45 C.F.R. § 5b.4 (2007).

²⁰HHS.Gov, About the Privacy Rule, <http://www.hhs.gov/hipaafaq/about/354.html>(last visited May 25, 2012).

²¹ INSTITUTE OF MEDICINE OF THE NATIONAL ACADEMIES, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, 1 (National Academy of Science 2009).

PHI.

- Create a mechanism for linking an individual's data from multiple sources such as databases so that more useful datasets can be made available for research in a manner that protects privacy, confidentiality, and security.
- All health research institutions [should] take strong measures to safeguard the security of personally identifiable health information.
- Support the development and use of new security technologies and self-evaluation standards.²²

The Commission should incorporate IOM's recommendations to strengthen privacy protections for genomic information.

We note also that as efforts are underway to update frameworks for privacy protection outside of the United States, greater attention is now given to the collection and use of genetic information. For example, a proposed change to Article 6 of the Council of Europe Convention 108, a widely recognized international instrument for privacy protection, incorporates the category of genetic data, which is also viewed as sensitive information.²³ In similar fashion, the recently proposed EU General Data Protection Regulation, which would take the place of the EU Data Protection Directive, also establishes new safeguards for genetic information.²⁴ Under both the revised Council of Europe Privacy Convention and the proposed EU General Data Protection Regulation, individuals would be given extensive control over the collection, use, and disclosure over their genetic information. Independent authorities would assess data practices, and fines

²² *Id.* at 2-3.

²³ Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997), available at <http://www1.umn.edu/humanrts/instree/coerecr97-5.html>

²⁴ Commission Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), at 62-63, COM (2012).

would be available when genetic information is not used for or its intended purpose or fairly processed.

The proposed revisions to well-established privacy frameworks provide additional guidance as the Commission considers the development of privacy policies for genetic information.

II. The Federal Government Should Control Access to Genomic Information

The Commission requested comments on “who should have access to [genomic] data and who should control access” to the data.²⁵ EPIC strongly recommends that the federal government control access to this highly sensitive information to ensure accountability, oversight, and transparency. For example, the Privacy Act of 1974 forbids federal agencies from disclosing “any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”²⁶ In certain limited circumstance, the Privacy Act permits disclosure of individual records without first obtaining individual consent. Individuals that release their genome data to the federal government should be fully apprised of their rights under the Privacy Act. Because of the particularly sensitive nature of human genome data, once agencies collect genomic information and it is placed within a system of records pursuant to the Privacy Act, agencies should not be permitted to exempt the system of records from Privacy Act requirements. Additionally, the genomic information should be exempt

²⁵ 77 Fed. Reg. 18247.

²⁶ The Privacy Act of 1974, Pub. L. 93-579, 5 U.S.C. § 552a (b)(2012).

from 5 USC § 552a(b) of the Privacy Act, which permits agencies to disclose information without written consent.

The federal government should control access to genomic information because the federal government is subject to FOIA oversight.²⁷ Through the FOIA, members of the public can monitor large-scale human genome sequencing research methods and agency policy. Oversight of the collection and use of genomic data is imperative to prevent potential data misuse and unauthorized data access. Should the private sector control access to genomic information, it could collect, sell, and access sensitive genomic information with limited oversight. The FOIA can help to ensure that government agencies abide by the Commission’s proposals and regulations concerning genetic data.

Moreover, many federal human research programs are subject to the “Common Rule.” Based partially upon the 1979 Belmont Report, which provided guidelines for ethical research in the biomedical and behavioral sciences, the Common Rule requires that “[f]ederally funded investigators in most instances obtain and document the informed consent of research subjects, and describes requirements for institutional review board (IRB) membership, function, operations, research review, and recordkeeping.”²⁸ Since its inception, fifteen federal departments and agencies have codified the Common Rule in their agency regulations.

²⁷ The Freedom of Information Act, Pub. L. 89-554, 5 U.S.C. § 552 (2012).

²⁸ Advance notice of proposed rulemaking: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, Docket ID number HHS–OPHS–2011–0005, 76 Fed. Reg. 44512.

III. The Circumstances, if any, that Provide Law Enforcement with Access to Genetic/Genomic Information Should be Narrowly Tailored

As discussed above, genetic information and corresponding biometrics are truly unique identifiers. Law enforcement already possesses sweeping authority to collect and access personally identifiable information, oftentimes, with little accountability.

Although EPIC recognizes that genetic information could potentially be useful to further legitimate law enforcement objectives, those objectives should be narrowly tailored.

Moreover, as Professor Latanya Sweeney of Harvard's Data Privacy Lab notes, "inferences drawn from DNA information can be used to divulge the exact identities of the persons from whom the DNA originated."²⁹ The ability for law enforcement to match genetic information with specific individuals could permit unlawful and pervasive surveillance of individuals. Genetic database access by law enforcement also raises due process implications because law enforcement could access this information without probable cause or a search warrant, violating the Fourth Amendment. Additionally, nonconsensual access to genetic data could rise to prohibited self-incrimination under the Fifth Amendment. These threats to civil liberties are severe enough that law enforcement access to genomic data should be narrowly tailored.

Conclusion

EPIC commends the Commission for recognizing the privacy implications associated with human genome sequence data. EPIC does, however, strongly recommend that: (1) the Commission builds upon well-established genetic privacy laws and

²⁹ Malin, B. and Sweeney, L. *Determining the Identifiability of DNA Database Entries*, 7 JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION. 537, 537 (2000).

strengthens those protections; (2) the federal government control access to genomic information; (3) the federal government abides by fair information practices as it collects genetic information; and (4) in the event that law enforcement is provided access to genetic information, this occurs under narrowly prescribed circumstances.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Open Government Fellow