THE GEORGE WASHINGTON UNIVERSITY MEDICAL CENTER
WASHINGTON DC

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE
CENTER FOR DEMOCRACY & TECHNOLOGY

May 25, 2012

The Presidential Commission for the Study of Bioethical Issues
Office of the Secretary
Department of Health and Human Services
1425 New York Avenue NW, Suite C–100
Washington, DC 20005
info@bioethics.gov

Members of the Commission:

We respectfully submit the following comments in response to the Request for Comments on Issues of Privacy and Access With Regard to Human Genome Sequence Data.

Genetic Information

Although health information is generally considered to be sensitive, certain types of health information are typically perceived to have a higher level of sensitivity, and genetic information falls into this category. McGuire et al. have presented some of the factors that render genetic data "exceptional"—for example, its uniqueness, its predictive capability, its immutability, its history of misuse, and its impact on entire families versus just one individual.[1] Federal and state policymakers have responded to concerns about the privacy of genetic data in a variety of ways. For example, in 2008 Congress enacted the Genetic Information Nondiscrimination Act (GINA), which focuses on protecting individuals from discrimination by employers or health insurers on the basis of their genetic information.[2] Although the scope of GINA's protection is broad, the law does not apply to benefits such as long-term care, disability, and life insurance.[3] However, because GINA defines "genetic information" as information about an individual's genetic tests, as well as the genetic tests of an individual's family members or the manifestation of a disease or disorder in an individual's family members,[4] it prevents the use of family

[1] McGuire, A. et al. "Confidentiality, privacy and security of genetic and genomic test information in electronic health records: points to consider." *Genetics in Medicine*, Vol. 10, No. 7, July 2008, pp. 495-489.
[2] GINA, Pub. L. No. 110-233, 122 Stat. 881 (codified in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).
[3] GINA §§ 201-213.
[4] GINA § 201, 122 Stat. at 906.

medical histories in employment and insurance decisions in addition to genetic information about the individual.[5]

State laws regarding genetic information generally focus on protecting patients from the use of the information by health insurers to deny coverage, although some states have laws regarding genetic information that are broad enough to include the disclosure of information by health care providers.[6] These laws may apply solely to genetic testing, or more broadly to genetics-related information, such as family health history or inherited characteristics.[7] State laws related to genetic information also vary in their consent requirements. For example, some require an individual's consent for disclosures for treatment purposes, while others do not, and a small number of states require consent for the release of information for treatment purposes even in the case an emergency.[8]

Despite the variation in state law, it is clear that the legal environment surrounding disclosure of genetic information recognizes the sensitive nature of such information and increasingly is making attempts to protect it. Accordingly, the increasing prevalence of genetic information in individuals' health records may also increase our need to consider additional methods of protecting that information.[9] Massachusetts law, for example, requires that the identity of an individual who has received a genetic test be protected from disclosure by encryption or encoding.[10]

The failure of policymakers to enact sufficient protections for genetic data could have disastrous results, as demonstrated by the recent negative reaction of the public to databases of blood spots routinely collected from newborns. The blood spots are collected primarily for screening for heritable and congenital disorders, but a number of states have made them available for research purposes as well. Recently, two states (Minnesota and Texas) were forced to destroy valuable databases of blood spots routinely collected from newborns due to parental concerns regarding the lack of prior consent to collection and/or use of the blood spots.[11] In Texas, parents now have the right to opt out

---

[5] Office for Human Research Protections, U.S. Department of Health and Human Services. *Guidance on the Genetic Information Nondiscrimination Act: Implications for Investigators and Institutional Review Boards*, March 24, 2009. Available at: http://www/hhs/gov/ohrp/humansubjects/guidance/gina.html.

[6] Pritts, J. et al. "Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information," August 2009. AHRQ Contract No. 290-02-0015, RTI International. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_910326_0_0_18/DisclosureReport.pdf.

[7] *Id. See, e.g.*, Tex. Occ. Code 58.001(2007) and N.J. Stat. Ann. 10:5-47(a),(b) (2008).

[8] Pritts, *supra* note 6.

[9] Goldstein, M.M. and Rein, A.L., "Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis," September 2010. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950145_0_0_18/gwu-data-segmentation-final.pdf. Certain elements of the discussion in these comments are derived from arguments made in this whitepaper.

[10] MASS. GEN. LAWS ANN. ch. 111 § 70G (West 2009).

[11] Drabiak-Syed, K. "Newborn blood spot banking: approaches to consent." PredictER Law and Policy Update. Indiana University Center for Bioethics. March 12, 2010. Available at: http://bioethics.iu.edu/programs/predicter/legal-updates/newborn-blood-spot-banking/ (summary of issue

of having newborn blood spots retained by the state, and in Minnesota blood spots cannot be used for purposes beyond screening without parental informed consent.[12] A similar law requiring consent for use of blood spots is now pending in California.[13] While this example relates to the special case of newborns and parental consent, the privacy and personal trust concerns surrounding the collection and storage of genetic material could be equally as relevant to individuals in the case of adult specimens.

Privacy and health IT

Health IT has a greater capacity to protect sensitive personal health information than is the case with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing among health care system entities for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption and similar technologies can reduce the risk to sensitive data when a system is breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, the perpetrators will be detected and punished.

At the same time, the computerization of personal health information (including genetic information), in the absence of strong privacy and security safeguards, magnifies the risk to privacy. Tens of thousands of health records can be accessed or disclosed through a single breach. In the fall of 2010, for example, private medical data for nearly 20,000 emergency room patients at Stanford University Hospital were breached by a billing contractor.[14] Just the month before, Science Applications International Corporation (SAIC) reported a breach of personal medical information from 4.9 million military clinic and hospital patients due to a theft of back-up tapes from an SAIC employee's car. [15] Sadly, such incidents are all too common, with 435 breaches of greater than 500 patient records having been reported to the U.S. Department of Health and Human Services (HHS) since implementation of federal breach notification rules covering health care entities in 2009.[16]

The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a historic lack of enforcement of existing privacy rules by federal authorities, has deepened consumer distrust in the ability of electronic health

---

written before the Minnesota Supreme Court determined the blood spots in Minnesota should be destroyed); http://www.health.state.mn.us/news/pressrel/2012/newborn013112.html.

[12] *Id.*

[13] http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1251-1300/sb_1267_bill_20120327_amended_sen_v98.html

[14] Sack, K. "Patient Data Landed Online After a Series of Missteps." *New York Times*, Oct. 5, 2011. Available at: http://www.nytimes.com/2011/10/06/us/stanford-hospital-patient-data-breach-is-detailed.html?pagewanted=all.

[15] *Id.*

[16] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

information systems to provide adequate privacy and security protections.[17] Survey data consistently show the public supports health IT but is very concerned about the risks health IT poses to individual privacy.[18]

In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information.[19]

Many of the concerns surrounding patient choice and privacy in the HIT context are, in a sense, extensions of reservations patients currently have regarding their medical records in general. Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[20] Without appropriate protections for privacy and security in the healthcare system, people will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[21] Such privacy-protective behaviors include failing to seek care for sensitive medical conditions, asking health care providers to leave sensitive information out of a medical record, and traveling outside of an area to seek care.[22] According to a

---

[17] *See* http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[18] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005); study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006); Consumer Engagement in Developing Electronic Health Information Systems, AHRQ Publication No. 09-0081EF (July 2009). In the most recent survey conducted by the Markle Foundation, more than 80% of both the public and doctors surveyed said that requiring protections and safeguards for patient privacy was important. http://www.markle.org/publications/1443-public-and-doctors-agree-importance- specific-privacy-protections-health-it (January 2011). Similarly, the National Partnership for Women and Families concluded from its February 2012 survey that "[a]lthough people see great value in EHRs and have high levels of trust in their doctors, our findings indicate they are also wary that more widespread use of EHRs will lead to increased data breaches." *Executive Summary*, "Making it Meaningful: How Consumers Value and Trust Health IT." http://www.nationalpartnership.org/site/DocServer/HIT_Making_IT_Meaningful_Exec._Summary.pdf?docID=9784 (February 2012).

[19] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006).

[20] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[21] *Id.*

[22] *Id.*

2007 poll, one in six adults (17%) – representing 38 million persons – said they withhold information from their health providers due to worries about how the medical data might be disclosed.[23] A September 2011 study by the New London Consulting commissioned by FairWarning®, a vendor of breach detection software, found that:

- 27.1% of respondents stated they would withhold information from their care provider based on privacy concerns.

- 27.6% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.

- Greater than 1 out of 2 persons said they would seek care outside of their community due to privacy concerns, and 35% said they would drive more than 50 miles to seek care.[24]

The consequences of this climate of fear are significant—for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;

- Their health care providers' ability to diagnose and treat them accurately may be impaired;

- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and

- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[25]

Contrary to the views expressed by some, privacy is not the obstacle to great adoption of health IT. In fact, appropriately addressing privacy and security is key to realizing the technology's potential benefits. Simply stated, the effort to promote widespread adoption and use of health IT to improve individual and population health will fail if the public does not trust it. Because it is often difficult or impossible to establish effective privacy protections retroactively, we are now in the critical window for addressing the issue. Restoring public trust that has been significantly undermined is much more difficult – and more expensive – than building it at the start.

---

[23] Harris Interactive Poll #27, March 2007. Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy- protective behaviors. National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

[24] http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-US-PATIENT- SURVEY .pdf

[25] Protecting Privacy, supra note 20.

Individual Choice and Public Good

Policy decisions regarding how and to what extent patients exercise control over the electronic exchange of their health information have been discussed at times as representing the degree to which patient privacy and autonomy are preserved in a networked health environment. As both clinical and research medicine traditionally have relied upon informed consent to further the ethical principles of autonomy and self-determination in practice, the proper role of informed consent in electronic information sharing has been widely discussed in recent years.[26]

It has been suggested that an individual's participation in electronic health information exchange should be thought of as a type of medical intervention in which "one needs to balance the benefits of using the systems with the potential risks to the patient."[27] While a system that allows for greater patient control over his or her medical records may provide more choice to the individual patient, there is considerable uncertainty as to whether access to a range of choices ultimately satisfies the health interests of the individual patient and, more broadly, undermines the utility of the exchange for both the patient and society. In addition, it has been argued that over-reliance on consent could lead to "consent fatigue," where patients presented with too many complex consent forms unknowingly agree to uses and disclosures of their health information.[28] The concern is that a system that relies on consent alone to maintain patient choice and privacy paradoxically may subvert these goals by shifting the focus away from true autonomous choice and toward a legally binding, but ethically questionable, process that consists primarily of the mere signing of forms.

One important but confounding challenge in discussing consent's role in electronic health information exchange is taking into account the benefits that it promises on a societal scale. Encouraging individuals to seek care in the first instance by promising confidentiality helps fulfill the societal goal of having a healthy population. While electronic exchange of data has the potential to advance such societal goods as population health and clinical research, this effect diminishes as fewer patients participate and less data are available. These uses of health data promise benefits for both the individual and society, but their potential ultimately depends on the extent to which such data are made available for these purposes. While it does not necessarily follow that participation in electronic exchange should be mandatory, the overall costs and benefits to all participants must be considered in deciding consent's proper role in electronic exchange.[29] It has been noted that, at least in our current health care system, the individual, as opposed to

---

[26] Goldstein, M.M. and Rein, A.L. "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis," March 2010. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147. Certain elements of the discussion in these comments are derived from arguments made in this whitepaper.

[27] Berner, E.S. "Ethical and Legal Issues in the Use of Health Information Technology to Improve Patient Safety," *HEC Forum*, Vol. 20, No. 3, September 2008, pp. 243-58, at 244.

[28] Center for Democracy and Technology. "Rethinking the Role of Consent in Protected Health Information Privacy," January 2009, at 10. Available at: http://www.cdt.org/healthprivacy/20090126Consent.pdf.

[29] Goldstein and Rein, "Consumer Consent Options," *supra* note 26.

society as a whole, bears the primary risks associated with the improper use and disclosure of information, such as losing employment or insurance.[30]

Ultimately, striking a balance between enabling autonomy and patient choice and achieving socially fair and legally valid standards for medical (including genetic) data use and electronic exchange recalls the foundations of the doctrine of informed consent itself—meeting legal and professional standards of informed consent does not always fulfill the ethical obligation of maintaining patient autonomy. As health information becomes more complex and widely available, our societal challenge is to develop consent rules and procedures within HIT that honor the goal of autonomous choice while simultaneously acknowledging considerations of clinical efficacy, resource restrictions, and the greater social good.[31]

The Fair Information Practice Principles (FIPs)

The limitations of the mechanism of consent in protecting patient privacy have led many groups, including the Center for Democracy and Technology (CDT) and the Markle Foundation, to recommend integrating individual control and consent into a robust framework of legal, technical, and policy rules organized to protect the privacy and security of data.[32] Within this paradigm, they suggest that individuals should be informed about and agree with how their health information is being collected and used, but not rely on consent alone to bear the full weight of privacy protection.[33] Such frameworks are generally based on "fair information practices" (FIPs), a set of principles that have been relied on to define information privacy rights in a variety of contexts in the United States and internationally. The FIPs were developed in the United States in the 1970s[34] and have been both incorporated into sector-specific privacy laws and applied to the personal data that federal agencies themselves collect. In addition, the FIPs are a foundation for numerous international data privacy frameworks, including the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[35]

---

[30] *See* Pritts, J. "The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research," National Academy of Sciences, 2008. Available at: http://www.iom.edu/Activities/Research /HIPAAandResearch.aspx.

[31] Goldstein, M.M. "Health Information Technology and the Idea of Informed Consent," *Journal of Law, Medicine, and Ethics*, Vol. 38, No. 1, pp. 27-35.

[32] Center for Democracy and Technology. "Rethinking the Role of Consent in Protected Health Information Privacy," January 2009, at 10. Available at: http://www.cdt.org/healthprivacy/20090126Consent.pdf; Center for Democracy and Technology, "Beyond Consumer Consent: Why we Need a Comprehensive Approach to Privacy in a Networked World," *Markle Foundation*, February 2008 [hereinafter "Beyond Consumer Consent"]. Available at: http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

[33] Center for Democracy and Technology. "Beyond Consumer Consent," *supra* note 32.

[34] In 1973, the Department of Health, Education, and Welfare released the report, "Records, Computers, and the Rights of Citizens," which outlined a Code of Fair Information Practices that would create safeguard requirements for certain "automated personal data systems" maintained by the Federal Government.

[35] *See* U.S. Department of Commerce, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, at 9.

The FIPs implicitly acknowledge the need to collect and share information and to build trust in these necessary data flows through practical and workable rules. In the health context, they present a model of strong data stewardship, where entities that access, use, disclose or retain personal health information are subject to a set of obligations (imposed through law and the adoption of responsible business practices) that determine when they are permitted to collect, use, disclose and retain such information and the types of security safeguards that must be employed to bolster those policies. They include transparency about data policies; specifying the permitted purposes for collection, use and disclosure of health information and then placing limits on data flows consistent with these purposes; protecting the quality, integrity, and security of information collected; and ensuring accountability for compliance with data policies.[36] The principles balance patients' various and sometimes competing needs within the overall context of health and health care—for example, coordinating health care among patients and diverse providers, and accessing safety and quality data about providers and treatments for the public good, all while assuring the privacy and security of personal health information. Whereas consent alone cannot bear the entire burden of protecting personal data, a robust framework of legal, technical, and policy rules based upon the FIPs and organized to protect the privacy and security of data is more likely to achieve that goal.

Issues for Consideration by the Commission

a. Framework of protections for genetic data

In general, federal and state policy governing uses of genetic data requires informed consent or authorization before such data can be collected or disclosed—and this is particularly the case for research uses of genetic data. But given the limitations of consent as the sole protector of sensitive personal information, more emphasis should be placed on developing policies and best practices to implement the other fair information practices, which help ensure responsible use and stewardship of personal information regardless of whether or not an individual has been given the opportunity to consent. For example, limiting who has access to genetic information to only those individuals with a need to access the data, providing transparency regarding uses of genetic data, ensuring adequate security for genetic information and establishing robust systems of accountability for misuse or mishandling of genetic information will help build public trust in collection and uses of genetic data.

Available at: http://www.commerce.gov/blog/2012/02/23/us-commerce-secretary-john-bryson-delivers-remarks-unveiling-%E2%80%9Cconsumer-privacy-bill-. *See also* Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, March 26, 2012. Available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[36] *See* Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information," December 15, 2008. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy__security_framework/1173.

b. Should federal rules governing research allow for general consent to use genetic data for future research?

Recently, the Secretary of HHS and the Office of Science and Technology Policy released an advance notice of proposed rulemaking seeking public comment on potential changes to the Common Rule, which governs federally-funded human subjects research.[37] HHS is considering changes to the Common Rule that would allow individuals to provide a general consent to future research uses of biospecimens (which include genetic information).[38] The HHS Office for Civil Rights, which has oversight over the Health Insurance Portability and Accountability Act (HIPAA) privacy rules, has also proposed allowing individuals to provide general consent to research uses of their information.[39] From an ethical and legal standpoint, it is difficult to comprehend how individuals can give truly informed consent to future, undefined research uses of their sensitive health information. However, robust implementation of other fair information practices may bolster the protective value of such general consents. For example, if the potential research uses of genetic data are subject to objective review, and are made routinely transparent to the public, and there is strict accountability (such as through audit) to ensure compliance by researchers with good data stewardship practices, such a policy framework – even with only general consent – might achieve public acceptance. Piloting promising approaches – and assessing stakeholder satisfaction with the process and the results – could help pave the way to broader reform.

c. Should all "research" uses of genetic data always require consent?

With respect to secondary research uses of data initially collected for clinical purposes, some have recommended that, in pursuit of a learning healthcare system, federal regulators should consider narrowing the definition of what constitutes "research." In both the Common Rule and the HIPAA Privacy Rule, research is defined as an activity intended to "contribute to generalizable knowledge." Consequently, a health care entity covered by HIPAA may conduct an assessment of the quality of care provided without first obtaining the consent of the patient if the assessment will be used for internal purposes only. However, if the entity intends to share that same assessment with others to contribute to generalizable knowledge, the activity is regulated as research and subject to informed consent requirements if the data are identifiable and consent is not waived by an Institutional Review Board.

The federal Health IT Policy Committee, established in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to advise the Office of the National Coordinator for Health IT (ONC) on electronic health information exchange policy issues, has urged HHS to revise these rules to consider quality assessment and improvement initiatives using clinical data to be routine operations and not research, as long as fair information practices are followed. This would hold true

[37] 76 Fed. Reg. 44512 (July 26, 2011).
[38] *Id.*
[39] 75 Fed. Reg. 40868, 40893 (July 14, 2010) (HHS has not yet issued its final determination on this proposal).

even if the results are shared with others to contribute to generalizable knowledge.[40] CDT has also advanced this idea.[41]

The Commission could give further consideration to whether genetic data in clinical records – when used for purposes of assessing the quality of care delivered (such as examining whether the care provided to a person with a known genetic marker was provided consistent with evidence-based guidelines) – should also be categorized as routine operations and therefore not require consent, particularly when other safeguards (such as strictly limiting access to the data) are followed.

d. Can electronic health records used by providers honor consent requirements?

The laws of many states require prior individual consent before genetic information can be collected, used or disclosed, even for treatment purposes.[42] However, the electronic health records typically used by clinicians do not have the capability to mask or segment genetic information in a health care record.[43] Such masking or segmentation would allow for other health information to be shared even in circumstances where patients decline to consent for the sharing of genetic data in the record. Since electronic health records will be sources of information (including genetic information) critical to research, developing the capability to segment genetic data could also help further important research goals. ONC has launched a "data segmentation" initiative to pilot promising data segmentation technological approaches;[44] the Commission should closely monitor developments in this area.

e. Protecting genetic data from re-identification

The HIPAA Privacy Rule establishes a number of safeguards for research uses of identifiable health information, but information that qualifies as "de-identified" has a "very small" risk of re-identification and therefore is not subject to regulation.[45] (Similarly, the Common Rule regulates research only on human subjects, which includes identifiable information.) Data can be de-identified under the Privacy Rule using a safe harbor method (which requires the removal of 18 categories of identifiers), or by having a

---

40 http://healthit.hhs.gov/portal/server.pt?open=512&objID=1815&parentname=CommunityPage&parentid=37&mode=2&in_hi_userid=11673&cached=true (see letter of October 18, 2011).

41 "Paving the Regulatory Road to the Learning Health Care System," 64 Stanford Law Review Online 75 (February 8, 2012), http://www.stanfordlawreview.org/online/privacy-paradox/learning-health-care-system.

42 Pritts, supra note 6

43 The federal Health IT Policy Committee conducted a hearing on the capability of existing electronic health records to mask or segment data and concluded that a number of EHRs were developing promising technological approaches to segmentation but such approaches were not yet in widespread use. See letter of September 1, 2010, http://healthit.hhs.gov/portal/server.pt?open=512&objID=1815&parentname=CommunityPage&parentid=37&mode=2&in_hi_userid=11673&cached=true. *See also* Goldstein, "Data Segmentation," *supra* note 9.

44 http://wiki.siframework.org/Data+Segmentation+for+Privacy+Sign+Up

45 Center for Democracy & Technology, "Encouraging the Use of, and Rethinking Protections for, De-identified (and 'Anonymized') Health Data" (June 2009), https://www.cdt.org/paper/encouraging-use-and-rethinking-protections-de-identified-and-anonymized-health-data.

statistician attest that the data raises a very small risk of re-identification.[46] Whether genetic data is "de-identified" is unclear; the safe harbor method requires the removal of "biometric identifiers" and "any other unique identifying number, characteristic, or code,"[47] which arguably precludes genetic data from qualifying as de-identified under this methodology. However, the statistical method can also be used to de-identify a data set. Publicly available genetic databases are considered to be de-identified or anonymized[48] (although, since HIPAA covers only health care providers who bill electronically using standard codesets, health plans and health care clearinghouses, these databases are likely not subject to the Privacy Rule, and, as far as we are aware, there are no specific standards for de-identification or anonymization in the Common Rule or any other provision of federal law).

However, even when data is de-identified according to HIPAA Privacy Rule specific standards, there remains a risk of re-identification, and genetic information is highly susceptible to re-identification.[49] To protect genetic data that is presumed to be de-identified or anonymized, the Commission should explore requiring recipients of such data to commit to not re-identifying the data. In this scenario, even recipients of publicly available data should be required to make this commitment as a condition of receiving the information. The Commission could also consider calling for federal legislation making it unlawful to re-identify genetic data obtained on the basis that the data is de-identified (with authority given to federal regulators to create any necessary exceptions for health or safety). Of note, the Federal Trade Commission, in a 2012 report on consumer privacy, suggested that robust, fair-information-practices-based privacy guidelines need not apply to "reasonably de-identified data," but only if the data were sufficiently protected from re-identification by downstream recipients.[50] This is sound public policy that should also apply to uses of presumably de-identified genetic data.

Conclusion

The balancing of individual and societal interests in privacy and data access are issues currently being debated throughout our society, within both the private and public sectors. We urge the Commission to consider the comments we have made within the context of this debate, as your deliberations will provide a unique perspective to policymakers at a critical time in the development of national electronic health information exchange. Thank you for the opportunity to submit these comments and we look forward to reviewing your findings and recommendations.

---

[46] 45 CFR 164.514(b).
[47] 45 CFR 164.514 (b)(2)(i)(P) & (R).
[48] McGuire, A. & Gibbs, R. "No Longer De-Identified," Science, vol 312, 21 April 2006, pp 370-71.
[49] *Id.*
[50] Federal Trade Commission, *supra* note 35.

Sincerely yours,

Melissa M. Goldstein[51]
The George Washington University

Deven McGraw[52]
The Center for Democracy and Technology

[51] Melissa M. Goldstein, is an Associate Professor in the George Washington University School of Public Health and Health Services. Professor Goldstein's recent research and writings have focused on privacy and security issues in health information exchange and the effects of health information technology on the physician-patient relationship. During the 2010-2011 academic year, Professor Goldstein served as a senior advisor to the Chief Privacy Officer in the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services.

[52] The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive, workable privacy and security policies to protect health data as it is exchanged using information technology. CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. Deven McGraw, as director of the Health Privacy Project, has testified before Congress five times on the privacy and security issues raised by health IT, and chairs the privacy and security policy working group of the federal Health IT Policy Committee (called the "Tiger Team").