ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

To The Department of Health and Human Services, Office of the Secretary, and Food and Drug Administration

Regarding the 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

Via Regulations.gov

October 26, 2011

The Electronic Frontier Foundation (EFF)[1] and Patient Privacy Rights (PPR)[2] appreciate the opportunity to comment on the Advance Notice of Proposed Rulemaking (ANPRM) on human subjects research protections that appeared in 76 Federal Register 44512 (July 26, 2011). Accordingly, these comments mostly address privacy issues raised by the ANPRM.

Summary

With respect to biology and medicine, the ANPRM overemphasizes research at the expense of human subjects' privacy and autonomy, and robust informed consent mechanisms are necessary (though not sufficient).

These privacy concerns are especially great with respect to biospecimens.

The Department must recognize, however, that human subjects research in the field of computer science differs significantly from such research in biology and medicine.

Overview

We appreciate the ANPRM's effort to impose greater privacy and security protections overall, but remain extremely concerned about preserving and improving privacy protections for individuals as government and industry push for greater electronic exchange of health information. Increased digitization generally speeds data movement and increases data concentration, creating greater risks to information privacy and security.

Individuals value their privacy, and patients are nervous about how digitization will lead to increased sharing of their health information. One study found that 42 percent of those surveyed were uncomfortable with electronic health record sharing even if name, date of birth, address, and Social Security Number would not be shared and another 25 percent

[1] EFF is an active participant in policy dialogue in areas such as health privacy and computer science research privacy.
[2] Patient Privacy Rights is the nation's leading health privacy watchdog and leading consumer voice for building ethical, trustworthy HIT systems. For more information, visit: http://patientprivacyrights.org/.

454 Shotwell Street • San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org information@eff.org

were not sure, while 15 percent who knew their information would be shared would hide information from their doctor and another 33 percent would consider hiding information. *Consumers and Health Information Technology: A National Survey*, California HealthCare Foundation 24-25 (Apr. 2010), http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey. Another study found that a majority of the public believes that medical data is "no one else's business" and ought not be shared without their permission as "a matter of principle." AHRQ Publication No. 09-0081-EF, *Final Report: Consumer Engagement in Developing Electronic Health Information Systems*, (July 2009) http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf.

Americans generally do not understand how their data is collected, used and disclosed, however. Indeed, EFF's experience with the California health privacy policy process showed that even medical professionals are only vaguely aware of how patient data moves in the complex modern healthcare system. http://www.cdph.ca.gov/programs/cclho/Documents/OHIIFlowMapsforLabDataeprescribingandEmergencyDeptData.pdf.

Americans also lack knowledge about the rules that govern the privacy and security of their personal data. A majority of consumers mistakenly believe that the mere presence of a privacy policy at an online site means that the site cannot share data with a third party.[3] It is therefore highly likely that many patients mistakenly believe that the physician-patient privilege of confidentiality or laws such as HIPAA strongly protect the privacy of their data.

These considerations justify maintaining informed consent as a cornerstone of the Common Rule. And if the Belmont Report's value of respect for persons is to be sustained, the Department must also recognize that privacy includes far more than informational risks. In the medical context, this aspect of privacy may be thought of as patient autonomy, but it also implicates patient trust in doctors and researchers. As the President's Council of Advisors on Science and Technology recently recommended:

> To build and maintain the public's trust in health IT requires comprehensive privacy and security protections that are based on fair information practices and set clear rules on how patient data can be accessed, used and disclosed, and that are adequately enforced. An individual's right to have some meaningful choice in how their information is shared is one important component of a comprehensive set of protections. Where such choices are provided, either in law or by policy, they must be persistently honored.

---

[3] *See* Chris Jay Hoofnagle, *What Californians Understand about Privacy Online* (2008), at http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1262130_code364326.pdf?abstractid=1262130.

PCAST, Report to the President, *Realizing the Full Potential of Healthcare Technology to Improve Healthcare for Americans* 46 (Dec. 2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

The stakes are even higher with biospecimens, which create special privacy risks. Not only is DNA analysis becoming much cheaper, and the ability to identify de-identified data and biospecimens greater, commercial demand for all types of data is growing under the rubric of "big data." *See, e.g.,* Quentin Hardy, *The Big Business of "Big Data,"* http://bits.blogs.nytimes.com/2011/10/24/big-data/. The recent U.S. Supreme Court case, *Sorrell v. IMS Health*, illustrated the appetite of pharmaceutical companies for patient prescribing data.

It is therefore disturbing that the ANPRM only once refers to the ethical issues surrounding Henrietta Lacks, and never mentions the Havasupai litigation[4]—surely cautionary tales in the field of research ethics. As one writer put it, "A significant segment of the public harbors a deeply rooted mistrust of medical research. They do not trust physicians and scientists to be open and honest with them. They fear that the privacy of their medical records will not be respected. They believe that someone somewhere is making a lot of money off of drugs and biological products that were developed using pieces of tissue from people who now are entitled to a piece of the profits. *The Immortal Life of Henrietta Lacks* speaks to that skepticism, and above all is the vivid testament of how the Lackses feel they've been treated by physicians, researchers, journalists, and corporations." Dale Keiger, *Immortal Cells, Enduring Issues*, Johns Hopkins Magazine (June 2, 2010), http://magazine.jhu.edu/2010/06/immortal-cells-enduring-issues/

EFF's concerns about the ANPRM extend beyond medical privacy, however. The ANPRM ignores that much federally funded computer research is now covered under the Common Rule. Today, research in computer security, usability, social networks, and many other areas relies on either explicit or implicit user studies. These fields have made considerable effort to operate within the Common Rule; indeed, the Department of Homeland Security has been working with researchers and privacy advocates (including EFF) on ethical guidelines for computer science and network research. *See, e.g.*, https://www.nsf.gov/events/event_summ.jsp?cntn_id=121875&org=NSF (discussing *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research* (work-in-progress)).

---

[4] *See, e.g.*, Amy Harmon, *Indian Tribe Wins Fight to Limit Research of Its DNA*, New York Times (April 21, 2010), at http://www.nytimes.com/2010/04/22/us/22dna.html. Also relevant is the controversy over newborns and bloodspots. Emily Ramshaw, *DNA Deception, DSHS Turned Over Hundreds of DNA Samples to Feds*, Texas Tribune (Feb. 22, 2010), at http://www.texastribune.org/texas-state-agencies/department-of-state-health-services/dshs-turned-over-hundreds-ofdna-samples-to-feds/.

Informational risks

The ANPRM views informational risks too narrowly. Informational risks are not limited to inappropriate use or disclosure of information. The compilation of personal information by a record keeper (who may or may not be acting with the knowledge and consent of a data subject) exposes the data subject to informational risk *regardless of the use and disclosure rules that apply*. Confidentiality privileges may be lost when data is transferred to researchers. Also, some disclosures are beyond the control of any record keeper. Any litigant or agency with a subpoena and any law enforcement officer with a search warrant may be able to force information disclosure, regardless of the record keeper's disclosure policy.

More generally, as noted above, privacy is not just about informational risks or avoiding informational harm. In the medical context, it is also about respect for persons and maintaining or creating patient trust.

Question 1: Is the current definition of ''minimal risk'' in the regulations (45 CFR 46.102(i) – research activities where ''the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests'')– appropriate? If not, how should it be changed?

Response: The Common Rule's concept of minimal risk should not apply to informational risks. Privacy risks *ordinarily encountered in daily life* are significant, poorly understood, and often hidden from view. Current debates over the use of information about Internet or cell phone users illustrate the point. Regular news reports highlight novel and often-secret data collection methods used by commercial companies in the pursuit of consumer profiles, more effective advertising, or increased profits.[5] Studies show broad gaps in popular knowledge about privacy.[6]

---

[5] *See, e.g.*, Center for Digital Democracy, *Examination of Online Direct-to-Consumer Prescription Drug Promotion* (2011) (Comments to Food and Drug Administration) ("Ongoing tracking and targeting of health users across the digital marketing system is a major concern not only for patient privacy, but also because such data is used to better hone campaigns designed to influence consumers in a myriad of ways. Health marketers strive to harness the data collection and analysis capabilities of online advertising in order to foster greater demand for prescription drugs. Unfortunately, little information is currently provided on what is being collected from users of health-related sites and how such data are used."), at http://www.centerfordigitaldemocracy.org/sites/default/files/FDAComments062711final.pdf.

[6] *See* Chris Jay Hoofnagle et al, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (2010) ("42 percent of young Americans answered all of our five online privacy questions incorrectly. 88 percent answered only two or fewer correctly. The problem is even more pronounced when presented with offline privacy issues – post hoc analysis showed that young Americans

The ANPRM's approach to informational risks is also poorly suited to areas like computer science. Today, computer scientists can easily create experiments that use human subject data from 100 or even 1000 individuals by, for example, placing an advertisement on Facebook, Google, or Amazon's Mechanical Turk and directing people to a website. These experiments can involve downloading software to a research subject's computer, which might damage the subject's computer (either the data or the physical computer itself), turn on the camera or microphone, scan the hard drive for personal documents, provide this information to the experimenter, or even post the information on a public website. Such consequences might be intentional or accidental (the result of software bugs).

De-identification and re-identification

Question 54: Will use of the HIPAA Privacy Rule's standards for identifiable and de-identified information, and limited data sets, facilitate the implementation of the data security and information protection provisions being considered? Are the HIPAA standards, which were designed for dealing with health information, appropriate for use in all types of research studies, including social and behavioral research? If the HIPAA standards are not appropriate for all studies, what standards would be more appropriate?

Response: We are critical of the ANPRM's reliance on de-identification as a privacy safeguard. In the past few years, researchers Arvind Narayanan and Vitaly Shmatikov have revolutionized the field of re-identification. Based on their statistical research and techniques for re-identifying purportedly anonymous datasets, they conclude that "[t]he emergence of powerful re-identification algorithms demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data." Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information,"* 53 Comms. of the ACM 24, 26 (2010); *see* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*. 29 Procs. of the 2008 IEEE Symp. on Security & Privacy 111 (2008); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1704 (2010). An important aspect of this problem is that re-identifiability is a function of both the putatively de-identified data set and other available data. Thus, it may be impossible to know if data is effectively de-identified, as a dataset that is de-identifiable today may become identifiable tomorrow, after more information is available.

Unsurprisingly, considerable research in the medical arena now focuses on the re-identification threat. *See, e.g.*, Grigorios Loukides et al., *Anonymization of Electronic Medical Records for Validating Genome-Wide Association Studies*, 107 Procs. of the Nat'l Acad. of Sci. 7898, 7902-03 (2010); Grigorios Loukides et al., *The Disclosure of Diagnosis Codes Can Breach Research Participants' Privacy*, 17 J. Am. Med. Informatics Ass'n 322, 322-23 (2010); Bradley Malin, *Re-Identification of Familial*

---

were more likely to answer no questions correctly than any other age group."), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. In other words, young and old alike did poorly on the test of privacy knowledge.

Database Records, Procs. of the 2006 Am. Med. Informatics Ass'n Annual Symp. 524, 528 (2006) (using online sources like newspaper obituaries and death records to link de-identified family relations to named people).

In addition, Congress never intended for HIPAA to set a federal ceiling, even in the health arena. As the Department stated in issuing the Amended Rule: "The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order to not interfere with such laws [affording a right of consent] and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a 'best practices' standard. Thus, professional standards that are more protective of privacy retain their vitality." 67 Fed. Reg. at 53,212 (August 14, 2002).

Question 56: DNA extracted from de-identified biospecimens can be sequenced and analyzed in other ways, with the results sometimes being linked to other available data than may allow a researcher to identify the persons whose specimens were being studied. How should Federal regulations manage the risks associated with the possibility of identification of such biospecimens? Should a human biospecimen be considered identifiable in and of itself? What are the advantages and disadvantages of considering all future research with biospecimens to be research with identifiable information?

Response: The re-identification problem is especially acute for biospecimens. NIH recently took steps to withhold from public disclosure *aggregate* genetic information that previously had been thought could not be individually identifiable.[7] While identifying a specimen today may still be difficult and expensive in many instances, the difficulty and expense of DNA analysis have been reduced enormously in the past decade. A recent report prepared for the U.S. Department of Defense predicts that the cost to sequence an entire human genome could drop to about $100 by 2013. JASON (The MITRE Corporation), *The $100 Genome: Implications for the DoD*, at 11 (Dec. 15, 2010).

The JASON report explains that while the first draft sequences of the human genome cost about $300 million, improvements in "second-generation" DNA sequencing platforms in the past five years have reduced the costs such that "[a]n entire human genome can now be sequenced in a matter of days for a retail cost of $20,000," and "third-generation"[8]

---

[7] *See* Homer N, et al., *Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays*, PLoS Genet 4(8): e1000167 (2008), at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2516199; *The National Institutes of Health removes patients' genetic profiles from its website after a study reveals that a new type of analysis could confirm identities*, LA Times (Aug. 29, 2009), http://www.latimes.com/news/nationworld/nation/la-me-dna29-2008aug29,0,4364552.story.

[8] The JASON report explains that "new technologies, called third-generation sequencing systems," are expected to account for this cost reduction. JASON 16. Technology being developed by Pacific Biosciences "should reduce reagent costs, increase read lengths, and dramatically reduce the time needed to sequence each nucleotide." *Ibid*. Another company, Ion Torrent, has developed advanced DNA sequencing chips that reduce costs

DNA sequencing technology will mean that "DNA sequencing costs will no longer be a factor limiting personal human genomics technologies." *Id*. at 2. Indeed, the cost "will likely fall to less than $1000 by 2012, and to $100 by 2013." *Id*. at 11 ("DNA sequencing technologies have advanced at a pace far greater than Moore's Law for transistor density"). Moreover, we cannot hide our DNA; we leave saliva on drinking glasses and skin cells everywhere. Thus, as genetic analysis becomes more prevalent, individuals require greater protection from informational and other risks.

We do not recommend that de-identification be abandoned. But given these trends, it is short-sighted to think that patient data, as a general matter, can be safely de-identified; de-identification should be treated as one precaution among many.

Regardless of these difficulties, de-identification under the "checklist" option of the HIPAA Privacy Rule (the "statistician" option is insufficient without greater oversight and accountability) is superior to the Common Rule's approach. Data that would be sufficiently de-identified for the Common Rule, e.g., by the removal of name, address and Social Security number, would not be de-identified under the Privacy Rule, which requires that all 18 data elements be removed.

Question 64: For research involving de-identified data, is the proposed prohibition against a researcher re-identifying such data a sufficient protection, or should there be in some instances requirements preventing the researcher from disclosing the de-identified data to, for example, third parties who might not be subject to these rules?

Response: In the biomedical arena, data use agreements that include overt third-party beneficiary clauses covering data subjects may be helpful.[9] However, blunt prohibitions on re-identification may create additional problems. As noted above, significant current research focuses on re-identification techniques that help us understand the risks of current de-identification techniques. The individual whose data is re-identified may not need protection against the statistical researcher who discovers a new re-identification technique and publishes an article about the technique in a scholarly journal, but does need protection against the banker, employer, insurer, and others who may seek to use re-identified data in ways that will affect the individual's interests. Moreover, blunt prohibitions on data re-identification (as opposed to biospecimens), especially involving

---

even though they are made with "chip fabrication facilities constructed in 1995"; "[d]ramatic" improvements "can be achieved simply by using more recent chip fabrication facilities, which effectively leverages the investments made to improve computer chip feature density to create massive improvements in DNA sequencing capability. Therefore, DNA sequencing chips that permit complete collection of a human genome for less than $100 seems within easy reach." Id. at 17-18.

[9] A brief discussion of the issue of third-party beneficiaries can be found at Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33, 50 (2010), at http://iplj.net/blog/wp-content/uploads/2010/11/C02_Gellman_010411_Final.pdf

publicly available data, may raise novel First Amendment issues that the Department should analyze before proceeding.

Informed consent

Question 45: Under what circumstances should future research use of data initially collected for non-research purposes require informed consent? Should consent requirements vary based on the likelihood of identifying a research subject? Are there other circumstances in which it should not be necessary to obtain additional consent for the research use of currently available data that were collected for a purpose other than the currently proposed research?

Question 46: Under what circumstances should unanticipated future analysis of data that were collected for a different research purpose be permitted without consent? Should consent requirements vary based on the likelihood of identifying a research subject?

Response: Unsurprisingly, the public favors strong consent requirements for research.[10] In one widely reported study, 38% agreed that "I would want each research study seeking to use my personally-identified medical or health information to first describe the study to me and get my specific consent for such use." Another 13% agreed that "I would not want the researchers to contact me or to use my personal or health information under any circumstances." Only 1% agreed that "Researchers would be free to use my personal health information without my consent at all," and only another 8% agreed that "I would be willing to give a general consent in advance to have my personally-identified medical or health information used in future research projects without the researchers having to contact me."

In commenting on this study, Dr. Mark Rothstein pointed out that "[a]mong the demographic groups reporting the greatest concern about the nonconsensual use of their health information are racial and ethnic minorities as well as persons with potentially stigmatizing and serious health conditions. Thus, members of vulnerable groups with a history of exploitation by researchers and those at risk from disclosure of their health information strongly disapprove of abandoning informed consent in information-based research." (footnote omitted).[11]

Rothstein emphasizes that the survey "also asked a follow-up question to determine the reasons why individuals would object to use of their health information for research without their consent. The number one reason — 77% — was: 'I would feel violated and my trust in the researchers betrayed.' This reason, outranking concerns about possible discrimination or embarrassment, underscores the notion that privacy is not the sole

---

[10] Alan F. Westin, *IOM Project Survey Findings on Health Research and Privacy* (October 2, 2007), at http://patientprivacyrights.org/media/WestinIOMSrvyRept.pdf?docID=2501

[11] Mark A. Rothstein, *Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark*, 37 J. L. Med. & Ethics 507, 511 (2009).

concern of individuals. Respect for persons and autonomy were of even greater importance."[12]

We therefore agree that informed consent requirements should apply to all research, but that the ANPRM's proposal is too weak. Under the ANPRM, written consent will be required for future research with material collected for non-research, e.g. treatment purposes, as well as for material initially collected for research purposes. For data collected initially for research purposes, merely oral consent for future research would be permissible if it was permissible for the initial collection. ANPRM, Table 1.

This is insufficient consent given the public desire for robust consent requirements. The HIPAA Privacy Rule requirements for *authorized* research, adequate or not, are stronger and preferable. Most important, the Privacy Rule provides that an authorization must, among other things, describe "each purpose of the requested use or disclosure." 45 C.F.R. § 164.508(c). The Department has long interpreted this provision to mean that an authorization must be related to a *specific* research study and *cannot* be used for future unspecified research. U.S. Dept. of Health and Human Services, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule* NIH Pub. No. 03-5388 (2003) ("Protecting PHI in Research"). HHS rejected the proposal to allow authorizations to encompass future research partially out of concern that individuals would lack the necessary information about future research to make an informed decision.[13]

The rise of genetic analysis raises additional consent issues, because of what a person's DNA reveals about family members. The 2003 European case *Gudmundsdóttir vs. Iceland* illustrates the issues. In that case, a young woman asked the Icelandic Ministry of Health not to transfer information in her deceased father's medical records, and any genealogical or genetic data on him that might exist, to Iceland's Health Sector Database, a national genomic database. Eventually, Ms. Gudmundsdóttir initiated legal proceedings, claiming that she had a personal interest in preventing the transfer of data from her father's medical records to the database because information relating her father's hereditary characteristics could also apply to her. The Icelandic Supreme Court not only held that she had standing to sue, but that the vagueness of the database's privacy protections inadequately protected her constitutional right to privacy. Her right to opt out of the transfer of her deceased father's health information was therefore affirmed.

Computer science research, especially network security research aimed at malicious attackers such as botnets, presents difficult informed consent problems because the researcher's only contact with the human subjects will be through the network and

---

[12] *Ibid*.

[13] The issue of what constitutes *informed* consent, of course, remains difficult. Too often, consent is viewed as an obstacle to be overcome, not as an essential part of a trust relationship—contrary to the spirit of the Belmont Report's principle of respect for persons, and perhaps lowering quality of care. *See* Schachter & Fins, *Informed Consent Revisited: A Doctrine in the Service of Cancer Care*, The Oncologist 2008;13: 1109–1113.

mediated by the subject's computer; these problems are beyond the scope of these comments, but are addressed by the previously mentioned *Menlo Report*.

Standards and protections

Question 58: Should the new data security and information protection standards apply not just prospectively to data and biospecimens that are collected after the implementation of new rules, but instead to all data and biospecimens? Would the administrative burden of applying the rule to all data and biospecimens be substantially greater than applying it only prospectively to newly collected information and biospecimens? How should the new standards be enforced?

Response: Leaving aside the content of the standards, we believe that they should apply to all data and biospecimens. It would be administratively difficult for most organizations to have privacy and security standards that apply to some research data but not to others. There may be a need for transition rules, especially for biospecimens, but the aim should be a single policy.

Question 59: Would study subjects be sufficiently protected from informational risks if investigators are required to adhere to a strict set of data security and information protection standards modeled on the HIPAA Rules? Are such standards appropriate not just for studies involving health information, but for all types of studies, including social and behavioral research? Or might a better system employ different standards for different types of research? (We note that the HIPAA Rules would allow subjects to authorize researchers to disclose the subjects' identities, in circumstances where investigators wish to publicly recognize their subjects in published reports, and the subjects appreciate that recognition.)

Response: Given the many different types of research subject to the Common Rule, including computer science research, we do not believe that the HIPAA Rules are appropriate across all contexts. In addition, the HIPAA Rules are far too lax with respect to disclosure of patient data to law enforcement and intelligence agencies. As noted earlier, HIPAA was intended to set a floor, not a ceiling, and should therefore be viewed as a starting point—not a destination.

Question 61: Are there additional data security and information protection standards that should be considered? Should such mandatory standards be modeled on those used by the Federal government (for instance, the National Institute of Standards and Technology recently issued a ''Guide to Protecting the Confidentiality of Personally Identifiable Information.'')?

Response: The basic idea of relying on existing models is a good one. However, the NIST document suggested is not a good example. By its own terms, the NIST recommendations "are intended primarily for U.S. Federal government agencies and those who conduct business on behalf of the agencies." Federal agencies and some federal contractors are subject to the Privacy Act of 1974, an old, largely outdated privacy law that cannot be readily applied in other contexts. The Act's use of a *system of*

records framework and its expansive disclosure authority make it inappropriate for broader application. Despite the Act's limited utility, Fair Information Practices (FIPS) are at the heart of the Act. FIPs should be used as the organizing policy for privacy under a revised Common Rule.[14]

In addition, we believe that meta-tagging patient information at a more granular level based on patient consent directives, together with a distributed cryptographic architecture in which data in transit and at rest are both encrypted (as suggested in the PCAST Report), is a promising direction that should be pursued. We are not, however, sanguine about the ability of technology to address these problems. Security in complex systems requires rigorous systems analysis involving understanding the complete flow of information as well the interaction of myriad system components.

We agree with other data privacy researchers such as Dr. Latanya Sweeney that the entire healthcare community must invest in data privacy research in depth. There is a crying need for greater transparency and accountability in the area of real-world patient data flows and commercial data collection, use, de-identification, sharing and re-identification practices.

Respectfully submitted,

Lee Tien
Senior staff attorney
Electronic Frontier Foundation

Deborah Peel, M.D.
Founder & Chair
Patient Privacy Rights

[14] For a history of FIPs, *see* Robert Gellman, *Fair Information Practices: A Basic History*, at http://bobgellman.com/rg-files/rg-resources.html.