



HIT POLICY COMMITTEE & HIT STANDARDS COMMITTEE
PCAST WORKGROUP HEARING
FEBRUARY 15, 2011
WRITTEN TESTIMONY OF THE ELECTRONIC FRONTIER
FOUNDATION
Lee Tien, Senior Staff Attorney

The Electronic Frontier Foundation (EFF) is grateful for the opportunity to provide written testimony about the PCAST Report. EFF is a non-profit, public-interest civil-liberties organization based in San Francisco, California. One of our principal missions is the protection of privacy in the information age, including patient privacy. To that end, EFF has been active in the California Office of Health Information Integrity's health information exchange policy development process.

EFF generally agrees with the Report's emphasis on the need to build greater privacy and security into the healthcare system, and its clear understanding that technology creates the opportunity to do so. We welcome its focus on patient consent and emphasis on patient consent directives. While robust consent mechanisms are not sufficient to protect patient privacy, they are definitely necessary.

Moreover, we generally agree that:

- A federated model of patient information stored locally is strongly preferable to creating centralized repositories of patient information;
- 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, is a promising direction that should be pursued;
- A universal health identifier should be rejected as unnecessary given the power of identity resolution mechanisms.

At the same time, however, we believe that the Report's recommendations for action raise many difficult technological and policy issues that need more concrete articulation and discussion.

In our view, patient care—"treatment," in the language of HIPAA—is the main, primary, predominant purpose of the healthcare system. Correlatively, privacy and security of patient information are essential if patients are to trust the healthcare system to provide quality treatment. This militates in favor of more constrained, rather than less constrained, dissemination of patient information for the foreseeable future. Patients should not be test subjects for an unproven system.

We are therefore troubled by the Report's emphasis on other goals, such as public health and medical research. While these goals are important, we believe that placing them on a par with patient care risks compromising the privacy and security needed for patient trust in the healthcare system.

The Report's attempt to balance these goals leads to apparent internal contradictions. Despite the Report's emphasis on privacy and security, it also emphasizes exchange in order to promote innovation and entrepreneurship. ("What is needed is a simultaneous focus on the capability for universal data exchange, able to unleash the power of the competitive market, to produce increasingly better and less expensive systems, and to create the 'network effect' that spurs further adoption" (p. 3); "We think that a universal exchange language must facilitate the exchange of metadata tagged elements at a more atomic and disaggregated level, so that their varied assembly into documents or reports can itself be a robust, entrepreneurial marketplace of applications." (p. 72)).

But if we do not know that exchange is secure, or that recipients of patient information will properly use that information, exchange will threaten patient privacy. Simply put, we believe there is a tension between velocity of exchange and privacy/security of patient information. We are thus greatly disturbed by this statement in the Report: "It seems likely that the modifications to HIPAA enacted in Subtitle D of the HITECH Act—in particular those that require covered entities to track all disclosures to associates—will further stifle innovation in the health IT field while offering little additional real-world privacy protection." (p. 48, footnotes omitted) We do not understand how the Report can propose strong audit trails for

decryption of patient information while criticizing the tracking of disclosures.

We also are not 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. By promoting an infrastructure geared toward information exchange for multiple purposes, we fear that the proposal will trend toward an inherently insecure system for which system analysis will be difficult, if not impossible.

In such a wide-open ecosystem, who would be responsible for analyzing the safety of software? The security vulnerabilities of standard commercial software, including common operating systems, are well known, and there is no good reason to believe that software in the healthcare industry will be any less vulnerable. Indeed, application software security depends to a large extent on operating system security—weaknesses in operating systems can undermine otherwise secure applications.

More generally, security for multiple-user, multi-level databases is an extremely hard problem. Patient data is sensitive over at least the lifetime of the patient, which means that privacy and security design must take a long view. Thus, while we find the Report's proposed architecture for patient data storage and cryptographic management attractive, it must be subjected to rigorous testing.

One important technical problem today, for example, is re-identification of supposedly de-identified data. Only in the last few years have we come to realize how difficult it is to truly de-identify data, given the enormous amount of information about people that is publicly available to data-miners, including hospital discharge summary databases. Modern re-identification techniques do not depend on personally identifiable information—any information that distinguishes one person from another can be useful. As Narayanan and Shmatikov explain, “advances in the art and science of re-identification, increasing economic incentives for potential attackers, and ready availability of personal information about millions of people” create an enormous privacy problem. (attached)

The re-identification problem may be especially difficult for genetic information. Indeed, genetic information raises significant issues for

traditional notions of patient consent, because of what a person's DNA reveals about family members. The 2003 European case *Gudmundsdóttir vs. Iceland* illustrates both 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.

To its credit, the Report recognizes the need for a strong legal and regulatory framework to ensure privacy and security. Unfortunately, we cannot say that such a framework of rules exists today. But even if it did, significant resources must also be committed to oversight and enforcement in order to create incentives for compliance. Strong audit trails will facilitate enforcement, but unless actors throughout the system perceive a credible threat of enforcement, strong audit trails will have little deterrent value.

Furthermore, we do not believe that technology can be agnostic here. Any technological design must be acutely aware of the human element and designed to confront those human-created risks, especially when the system appears to be designed to promote rapid sharing of large volumes of patient data and the recipients of that data are many and varied.

Among those risks are economic and other incentives to exploit patient information for non-treatment purposes. Data mining of prescription information, which features prominently in the pending U.S. Supreme Court case *IMS Health v. Sorrell*, is an obvious example.

Similarly, the Report speaks glowingly of personal health record (PHR) systems and cloud computing. We believe strongly in patients' control of their own medical records and information. But we also believe that unwarranted patient trust in today's patchwork quilt of legal and regulatory protections, as well as lack of sophistication about both the advertising ecosystem and the online information environment, may unknowingly

expose sensitive patient records or otherwise compromise patient privacy, as suggested by the recent incident involving PatientsLikeMe. Julia Angwin and Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, <http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html>.

We therefore need not only be sure that patients understand the risks, but that the system is designed to take account of how patients may fail to understand those risks. We must also consider how new technologies and new modes of exchange intersect with existing legal and regulatory understandings. Does common-law or statutory confidentiality of patient information change when it is stored in the cloud in a PHR? Patient consent and patient control must not mean that patients shoulder the full burden of protecting their own privacy in a vastly complex and technologically sophisticated environment.

Finally, there are important policy and constitutional issues around government access to and use of patient data, which will always be of interest to government, whether for law enforcement or other purposes. Examples include government attempts to obtain abortion providers' records, government access to patient genetic information given the well-known forensic uses for DNA, and government interest in background checks for government or government contractor employees. Only last year, for instance, the New Hampshire Supreme Court issued an opinion establishing special procedures for search warrants for privileged medical records held by hospitals. (*In re Search Warrant for Medical Records of C.T.* (2010)) (attached) The presence of public or governmental entities within the healthcare system itself complicates these issues further.

A healthcare information system should not be a surveillance system, and we should be acutely aware of the pressures to use it as such. Internet and other communications service providers have long been under pressure, both individually and as an industry, to design their systems to facilitate law enforcement activity and to create encryption "back doors."

To conclude: We reiterate our agreement with the Report's vision of decentralized patient information storage, privacy-tagged data elements, and a strong, distributed cryptographic architecture in which data in transit and at rest are both encrypted. Data segmentation, such as for especially sensitive mental health, reproductive health, and similar data, will thereby be

facilitated. In this way, appropriate information can be made available to appropriate staff without overbroad and unnecessary disclosures.

We differ with the Report in believing that the emphasis at this stage should not be on accelerating information exchange but rather on ensuring that information exchange is done safely with regard to privacy and security of patient information. Extreme caution is warranted. Health information technology must be subjected to the most rigorous, adversarial security testing on a staged basis, beginning with synthetic patient data. Similarly, we must be clear on the policy issues and tensions that will always put pressure on a system that holds highly sensitive, legally confidential information about every individual's life.

In short, we think that the healthcare information system should be designed primarily with patient care in mind. We are confident that the healthcare system, if properly designed toward the goal of patient care, will also yield significant benefits in public health and research. But the privacy and security of patient information must be validated at every step in development, and with a clear understanding of the threats to patient privacy.

Respectfully submitted,
Lee Tien
Senior staff attorney
Electronic Frontier Foundation