Comments Regarding California Office of Health Information Integrity Privacy and Security Steering Team's Law Harmonization Recommendations

July 20, 2012

The American Civil Liberties Union of California, California Family Health Council, Electronic Frontier Foundation, Privacy Activism, Privacy Rights Clearinghouse, and World Privacy Forum submit the following comments on the California Office of Health Information Integrity (Cal-OHII) Privacy and Security Steering Team's Law Harmonization Recommendations.

1. Introduction

We generally support Cal-OHII's goal of clarifying health privacy laws and making them more accessible to all California stakeholders. We recognize that California law in this area is scattered across many code sections and poorly mapped to HIPAA. Our concern, however, is that the current harmonization process is both substantively and procedurally risky. The main substantive risk is that harmonization will weaken existing privacy protections, forgo an important opportunity to strengthen privacy protections, or freeze the law so as to make it harder for California to respond to the privacy challenges of new health IT.

The procedural risks are closely related. Precisely because health privacy law is so complex, it is difficult for consumer and privacy advocates to fully understand the costs and consequences of harmonization. Even the Electronic Frontier Foundation (EFF), which has been part of the harmonization process, has found it difficult to explain and justify the harmonization recommendations to fellow consumer and privacy groups.

Cal-OHII needs more transparency and accountability if it wishes to claim with confidence that these recommendations have public support. For instance, under the federal Administrative Procedure Act's notice-and-comment rulemaking provisions, federal agencies develop new rules on a concrete administrative record that includes not only the agency's own research and thinking but also the written views of stakeholders, who themselves can introduce facts, experience and opinion. This process, which yielded HIPAA's Privacy and Security Rules, requires the agency to make its decisions based on a factual record, to consider and respond to public comments, and to articulate why the agency made important choices, thus promoting rational policy over political interest. We need a similar formal process for HIPAA harmonization efforts.

2. **The Law Harmonization Recommendations document and the process by which it was arrived at are opaque**.

   - **The section "Why Is the Change Needed?," which purports to explain the purpose of reconciling HIPAA and the CMIA, is either tautological or unclear.** The Privacy Steering Team (PST) states that it is concerned about the impact of new technologies on "consumer privacy and provider liability . . . that existing laws were never originally created to address." Resolving the discrepancies between HIPAA and the CMIA will, supposedly, solve the problem.

     We do not disagree that there are discrepancies between state and federal laws regarding the privacy and security of protected health information. Nor do we disagree that the law needs to be updated to address technological change. What the PST Law Harmonization Recommendations fail to explain, however, is *how* harmonization solves the problems that universal electronic health records will create. It also fails to explain why bringing California laws in line with HIPAA is preferable to creating stronger protections for Californians' medical records. Essentially, the document seems to say that harmonization is needed because it is needed.

   - **The Law Harmonization Recommendations are not understandable to advocates or members of the public in their current form, and a great deal more explanation is needed.** The recommendations do not explain the meaning of the laws and regulations the PST intends to harmonize—neither the HIPAA sections nor the corresponding sections of the CMIA. The document does not explain how or why the PST arrived at its recommendations.

     Perhaps most important, the PST does not explain in detail the consequences of harmonizing HIPAA and the CMIA to Californians. That is, what privacy standards will apply to their medical records and whether and how they will benefit from harmonization—or not. This is a question that needs to be answered, since HIPAA was conceived as a baseline of privacy protections and specifically does not pre-empt stronger state laws, like California's. We need clearer and better documented assurances that harmonization will not subtly undermine rights and remedies under existing law. We need litigation analyses to convince us that changes will not affect the ability of Californians to hold covered entities accountable. We observe that HIPAA provides no remedies to individuals at all.

     One possible addition to the harmonization document could include a column that indicated whether the proposed change was "more protective" or "less protective" in relation to current California privacy law, with an explanation of each determination in an appendix. This is one example, but there are different ways the harmonization document could be made more

understandable and comprehensive.

Along with addressing the question of the benefits of harmonization to individuals, the PST should be forthcoming about other beneficiaries. Is harmonization intended to benefit individuals, or is its primary purpose to remove the privacy "barriers" to the flow and uses of electronic PHI?

- **The harmonization process up to this point is poorly conceived.** Medical privacy at the beginning of widespread adoption of HIE is a critical issue. The laws that regulate it should not be developed in the dark. The PST's intentions regarding harmonization are unclear. Does the PST believe it is necessary simply because there are discrepancies between HIPAA and the CMIA? Because other states are doing it? Is the purpose to pave over differences between HIPAA and the CMIA and eliminate privacy "barriers" to HIE?

  The lack of clarity about the PST's operations and intentions does not encourage public participation. Nor does the absence of clear, point-by-point explanations of the content of sections of HIPAA and the CMIA, along with the reasons the PST believes they should be harmonized and the consequences of harmonization. As a privacy advocate member of the PST, EFF readily admits that it has relied heavily on analysis of both state and federal law provided by both Cal-OHII staff, information provided by legal and practical experts on the PST, and information from invited subject-matter experts. EFF has also seen firsthand that reasonable lawyers and experts often disagree about the meaning of California law and how it intersects with HIPAA.

  Up to now, the PST has done little to encourage public participation, nor has it provided the information the public needs to make that participation meaningful.

3. **What is the goal of harmonization?**

   - **Do no harm.** It is our understanding that HIPAA–CMIA harmonization is *not* intended to weaken existing privacy protections in California law. We nevertheless fear that harmonization may have the opposite effect of bringing California standards down to the HIPAA level and filling omissions in California law with weak HIPAA regulations. It is not possible to know from the PST's harmonization narrative what it has done to ensure that its recommendations do not weaken state law privacy protections.

     For example, Article I, Section 1 of the California constitution is a bulwark of state privacy law, but it is not clear that the PST did any constitutional

analysis in arriving at its harmonization recommendations. Consider the recommendation to adopt the HIPAA provision at 45 C.F.R. § 164.512(k)(2):

> (2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

This provision appears to allow any covered entity to disclose any health record to the CIA, FBI, NSA, and many other federal agencies that play a role in intelligence, counter-intelligence, and national security activities without a court order, without any procedural or substantive protections or barriers, and even without any request from the agency. Under this provision, a hospital could disclose any or all of its patient medical records to the CIA on the hospital's own initiative. A hospital could even allow the CIA or other federal agencies to access the hospital's health record system on a permanent basis.

Why is this recommended? How did the PST determine that existing law permitted this permissive disclosure? Did the PST consider whether the state constitutional right to privacy requires greater protections? Did it consider whether California should allow these disclosures without any standard or procedure—like a subpoena—to protect the privacy interests of patient? Because existing California law is more privacy-protective overall than HIPAA, the spirit of California law would be better served by a more privacy-protective approach to national security or intelligence disclosures—even if nothing in the letter of California law currently does so. We add that we perceive no benefit to either California patients or the promotion of HIE if this HIPAA provision is adopted.

Another example is the marketing provisions of HIPAA, as amended by HITECH. Neither HIPAA nor the CMIA is a model of clarity on what "marketing" means, and what is or is not permitted. The PST's narrative document adopts the HIPAA marketing rule. Are we to assume that it also adopts HITECH's changes to the marketing rule? If the recommendation is to adopt, where is the discussion of how HIPAA + HITECH is either equivalent to or better than the CMIA? Where is the analysis of whether the new—and not yet final—federal rules will restrict marketing or will actually allow more of it?

Both of these examples are simply examples, but they lead us to worry about the harmonization project generally. Part of the issue may be viewed as a tension between fidelity to text and fidelity of intent, most clearly expressed in state constitutional privacy law. Precisely because we expect that the

growing use of EHR and HIE exposes more patient data to more entities, and thus to more privacy and security risk, we believe fidelity of intent is appropriate.

That the recommendations may ultimately be translated into potential legislative language only heightens our concern. We have all worked on legislation, and we all know that good policy ideas can mutate greatly in a political process. In this context, clear and detailed documentation is necessary protection.

4. **What does it mean to "adopt" HIPAA?**

- **The recommendations do not explain what it means to "adopt" HIPAA.** The recommendations use the term "adopt" throughout, but do not explain what it means to adopt a HIPAA definition or rule. Does it mean to substitute the language and content of HIPAA for the language and content of each comparable California law for which the recommendation is to "adopt?" Is it the meaning of a HIPAA rule as currently set by federal courts? Since "adopt" is the operative verb and the fundamental purpose of harmonization, a clear understanding of its meaning and implications is essential.

- **Does adopting HIPAA into the CMIA diminish or eliminate California's authority over its health care privacy laws?** We're concerned that by adopting HIPAA, California will be ceding authority to bureaucrats in Washington to determine the meaning of California law. This abandons one of the key strengths of HIPAA: non-preemption of more privacy-protective state laws. Will adoption of HIPAA provisions cede authority to federal courts to determine what California statutes mean?

  Does harmonization make it harder for California to craft rules that are stronger than federal law? California has consistently been a policy leader on individual privacy; for example, it was the first state to have a data breach law and the first to apply it to medical records. Once harmonization is accomplished, will California be unwilling to rock the harmony boat and address new privacy concerns that emerge after HIE has been implemented?

  Consider one area where HIE could make it desirable to develop new law where none currently exists: re-identification of de-identified data. Leaving aside research-supported doubts about how de-identified such data actually is, it seems likely that as EHRs make enormous volumes of patient data easily accessible, demands for de-identified data for purposes we have yet to imagine will increase. Even current uses of de-identified data highlight the need to regulate re-identification. For example, some companies currently offer free EHR systems to doctors—a business model supported by monetizing de-identified data culled from those EHRs.

Another example is the business of drug detailing reports, sold to pharmaceutical companies by data miners like IMS, to assist drug salesmen in targeting doctors based on knowledge of their prescribing habits. IMS takes data that is encrypted by applications that IMS installs at the data source. IMS removes the identifying elements, but the data is still identified by a number and could therefore be easily re-identified. A patient's activities can be tracked over time to show other prescriptions filled for the number assigned to that patient, how long the patient takes a drug, and if a drug is discontinued or a new one prescribed. What IMS does to de-identify prescription data is apparently enough to satisfy HIPAA, as long as IMS obtains an expert's determination that the risk of individual identification is very small (very small is not defined). The HIPAA rule on this point uses very poorly defined standards. It opens the door to exploitation of patient records under a scheme where privacy protections rest on the opinion of an expert hired by those seeking to exploit those records.

If such practices continue and expand, a California policy that protects individuals from "de-identification" that still allows continuous tracking and that also strongly restricts re-identification, would be a good idea. Merely requiring entities to publicly disclose their de-identification methodology and their expert's analysis of the risk of individual identification could improve matters considerably. But would a post-harmonization California be willing to enact a regulation that exceeds HIPAA requirements? For that matter, would a post-harmonization California even contemplate a far more fundamental shift in the data management paradigm: enhancing individual privacy by adopting technologies that enable personal control and management of medical information, as opposed to control by institutions and organizations?

5. **Does harmonization take into account the changes that HITECH will make once the new regulations are published?**

   - **HITECH is not mentioned in the narrative.** Are we to assume that whatever changes HITECH makes to HIPAA will simply be absorbed into the HIPAA rules that the PST recommends adopting?

6. **Conclusion**

In general, we are not reassured that either the process of developing these recommendations so far, or the goal of the process, is to strengthen privacy protections for Californians' medical information. We fear that greater consideration has been given to enabling adoption of HIE by providers and payers, than to the impact of HIE on the privacy of individuals.

Patient trust is critical to acceptance of HIE, because of the great sensitivity of individual health information. We believe that the current law harmonization process does a poor job of promoting public trust. The very real risk, from a

consumer/patient perspective, is that harmonization will be a closed-door, industry-dominated process that lacks both political legitimacy and policy rationality. We hope that these comments will help improve that process going forward.

Respectfully submitted,

ACLU of California
(http://www.acluca.org/)

California Family Health Council
(http://www.cfhc.org)

Electronic Frontier Foundation
(http://www.eff.org)

Privacy Activism
(www.privacyactivism.org/)

Privacy Rights Clearinghouse
(http://www.privacy.org)

World Privacy Forum
(www.worldprivacyforum.org/)