ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

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

July 20, 2012

By electronic mail

California Office of Health Information Integrity
1600 9th Street
Sacramento, CA 95814

attn: Kerry Cataline and Terry Meeker
California's Office of Health Information Integrity

re: Consumers Union's and Center for Democracy & Technology's Comments on The Privacy and Security Steering Teams' Law Harmonization Recommendations

Members of the Privacy Steering Team, the Security Steering Team, and the California Office of Health Information Integrity:

Consumers Union[i] and the Center for Democracy & Technology[ii] provide comment on the Privacy and Security Steering Teams' Law Harmonization Recommendations.

Last year, before CDT became a member, the PST embarked on an effort intended to harmonize the Health Insurance Portability and Accountability Act (HIPAA) and the Confidentiality of Medical Information Act (CMIA) in order to reduce actual and perceived conflicts, confusion, and inconsistencies presented by the two sets of health privacy standards. The PST's plan is to submit final recommendations to CalOHII, who will then submit them to the state legislature as a proposed amendment to the CMIA.

CU and CDT strongly support efforts to make privacy and security policy in California clearer and more comprehensive. Such efforts are critical to securing public trust in the use of HIT to improve individual and population health.

However, we share some of the concerns expressed by other consumer and privacy advocates about the harmonization project. As explained in more detail below, we believe the project will achieve its goals only if it is more focused and more transparent to the public.

CU and CDT are troubled by insufficient public transparency about the initiative and the significantly limited opportunities for input by other stakeholders. While the PST's meetings are available on webcast, the PST has not done an effective job of ensuring that a broad spectrum of stakeholders participates regularly in deliberations. By way of example, CDT, before being appointed to the PST, called in to several

meetings and was often unable to follow the meeting due to both technical problems and a failure by the PST to make documents and drafts publicly available, either in advance of or during the meeting. In addition, the PST has not made all of its deliberations open to the public or available for public inspection and comment; nor have there been accessible, public announcements for the formation of "Task Groups" that the PST solicits for areas where specialized expertise is deemed important. As a result, important stakeholders, many of them seeing the draft recommendations for the first time, are confused about the intent of the recommendations and uncertain about their merit.

CU and CDT are also concerned that the current draft recommendations are not accompanied by clear explanations of the reasons supporting each recommendation. As a result, patients, consumers and other stakeholders do not have a clear understanding of the perceived need for the recommended change and consequently have limited information with which to evaluate it. As a simple example, we point to the definitional changes of the recommendations in the first phase of the harmonization project. The PST recommends adopting HIPAA's 'business associate' definition and removing the term 'contractor' that is currently used by the CMIA. However, the PST gives no explanation of the perceived need for the change; what if any benefits there would be to adopting the HIPAA business associate standard; which, if any, additional entities will now be regulated by the CMIA; and which, if any, entities may no longer be covered by the CMIA following the adoption of the new standard. Put simply - what would this change mean and how will it affect relevant stakeholders, especially patients and consumers? The HIPAA Privacy Rule and the CMIA have been working together in California for many years, for both paper-based and electronic exchanges of personal health information, so stakeholders need such explanations in order to evaluate the recommended changes.

CU and CDT believe that it is possible to refocus the harmonization initiative and build in sufficient public transparency and collaboration to ultimately achieve the worthwhile goals of the project, and as a new member of the PST, CDT is committed to helping to resolve these issues.

We suggest that PST refocus its efforts by more carefully examining existing privacy and security law in California and identifying clear gaps and areas of confusion that need to be addressed. This examination should be a public process, with opportunity for public comment, so that the ultimate "roadmap" for the harmonization process is one that has built and achieved broad public understanding and support. For example, the PST could initially consider addressing areas or issues for which there are currently no legal standards or safeguards for personal health information, or areas where current policies are not well understood or insufficiently enforced. Such policy gaps allow for the use and transfer of personal health information in ways that could undermine public trust, creating an environment where individuals do not feel safe or confident utilizing HIT tools. Specifically, CU and CDT believe the following issues could be the subject of focus by the PST:

- All business entities that access, use, and disclose personal health information should be held accountable for complying with comprehensive legal obligations to protect health data. Today, federal coverage under HIPAA is limited to traditional health care system entities (e.g., providers and insurers) and their contractors (business associates). California lawmakers recently extended the CMIA's scope, but it is unclear whether these expansions suffice to provide comprehensive protections for consumers and patients regardless of which entity is accessing their information.
- Accountability for compliance with federal and state health privacy and security protections should be strengthened. Lack of effective enforcement of existing law undermines the public's trust in holders and users of personal health information. At the same time, enforcement policy at both federal and state levels must be robust without making health care entities so overly cautious that they fail to share information in ways that facilitate the provision of good health care, both at an individual and population level.
- Laws that protect electronic health data, such as the HIPAA Security Rule, should be reassessed to ensure that they are sufficient to meet new security challenges and to incorporate technological innovation. For example, reports of data breaches filed with the HHS Office for Civil Rights, which enforces the breach notification requirements under HIPAA, strongly suggest that entities covered by these rules are not consistently using encryption to protect stored health information. Encryption is one of the core protections that electronic health records and information exchange make available.
- Rules on the use of personal health information for marketing purposes should be strengthened. Survey data demonstrate that this remains a persistent concern of consumers. Congress enacted provisions in the HITECH Act to strengthen federal rules on the use of personal health information for marketing purposes, but two years later, regulations to implement those provisions have not been finalized and could instead weaken them.
- Policymakers should provide more clarity on how entities are expected to comply with existing and new health privacy laws. Entities that are uncertain about whether they can use and share information lawfully may err on the side of caution and decide not to share. In circumstances where sharing should be encouraged, such uncertainty could be an obstacle to progress in leveraging data to improve individual and population health.
- Policymakers should ensure that standards for de-identifying health data remain robust and should establish penalties for inappropriate or unauthorized re-identification.
- Where possible, data-sharing models that favor decentralization and local control should be prioritized in lieu of duplicate databases created each time health information is needed for a particular purpose. Duplication and centralization of data amplify the risk of security and privacy violations.

> Local control also builds upon existing infrastructures (augmented as necessary to adhere to privacy and security standards, to ensure interconnection and interoperability, and to incorporate innovations), so that the benefits of HIE are realized more quickly.iii

As the PST and SST move forward with the harmonization process, it will be critical to be open and transparent at every step in the process. This includes providing detailed explanation of what legal standard each recommendation will specifically change, how the legal standard will be changed, and a justification or the rationale behind the recommendation. Including this additional information will allow patient/consumers, their advocates and the public the ability to formulate informed judgments on the changes, engage more significantly in the process, and feel confident that their privacy and security rights are being enhanced and not reduced.

Health information exchange should be built on institutional trust, bolstered by a comprehensive privacy and security framework that details clear policies regarding how data can be used and disclosed. The work PST is doing to build this framework should be continued. CDT is committed to helping the PST achieve a strong policy framework protecting health data.

We thank our fellow members of the PST, SST and CalOHII for the opportunity to issue these comments.

Respectfully,

Mark Savage
Consumers Union of
United States

Deven McGraw
Kate Black
Center for Democracy
& Technology

Attachment

---

[i] Consumers Union of United States, Inc., publisher of Consumer Reports7, is a non-profit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health, and personal finance. Consumers Union's publications have a combined paid circulation of approximately 8.3 million. These publications regularly carry articles reporting on Consumer Union's own product testing; on health, product safety, and marketplace economics; and on legislative, judicial, and regulatory actions that affect consumer welfare. Consumers Union derives its income solely from the sale of Consumer Reports7, its other publications and services, fees, noncommercial contributions and grants. Consumers Union's publications and services carry no outside advertising, and Consumers Union does not accept donations from corporations or corporate foundations.

[ii] The Center for Democracy and Technology ("CDT") is a non-profit Internet and technology advocacy organization located in San Francisco, California, and Washington, D.C., which promotes public policies

that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. CDT plays an instrumental role in safeguarding consumer privacy on the Internet. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

[iii] See "Achieving the Right Balance: Privacy and Security Policies to Support Electronic Health Information Exchange," California HealthCare Foundation Issue Brief (June 2012), written by Consumers Union and the Center for Democracy & Technology, http://www.chcf.org/publications/2012/06/achieving-right-balance (attached).