Consumers Union
Nonprofit Publisher of Consumer Reports

December 1, 2009

By U.S. mail and electronic mail

Secretary S. Kimberly Belshé
California Health and Human Services Agency
1600 Ninth Street, Room 460
Sacramento, California 95814

RE: CONSUMERS UNION'S AND CENTER FOR DEMOCRACY AND TECHNOLOGY'S COMMENTS UPON DRAFT INTERIM PRIVACY AND SECURITY GUIDELINES FOR HEALTH INFORMATION EXCHANGE IN CALIFORNIA, RELEASED OCTOBER 20, 2009

Dear Secretary Belshé:

Consumers Union[1] and Center for Democracy and Technology[2] write to express our concern about some language in the draft Interim Privacy and Security Guidelines ("draft Guidelines") and the motions of the California Privacy and Security Advisory Board at its meeting on September 16, 2009. Patients want better health care through the

[1] Consumers Union of United States, Inc., publisher of *Consumer Reports*, 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 has approximately 8.3 million paid subscribers to its publications, services and products. These publications regularly carry articles reporting on Consumer Union's own product testing; health, product safety, and marketplace economics; and legislative, judicial, and regulatory actions that affect consumer welfare. Consumers Union derives its income solely from the sale of *Consumer Reports*, its other publications and services, fees, and noncommercial contributions and grants.

Consumers Union's mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. In line with that mission and our assessment of priorities, Consumers Union has actively worked for a fair and just marketplace for patients and consumers in health care, health information exchange, patient safety, and health evaluation and rating of health services. Consumers Union has been extremely active in these areas both to improve the quality of health care for patients and consumers, and to inform consumers and to advocate for consumers before Congress, state legislatures, and regulatory agencies.

[2] 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.

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

use of health information technology and exchange, and they want to ensure that their data are protected by an appropriate set of privacy protections. Measures we adopt to protect privacy should promote both goals.

Specifically, we are concerned about the meaning or effect of language in both the draft Guidelines and the Advisory Board's motions regarding uses and disclosures for "health information exchange." Some language uses "health information exchange" as a *noun*, meaning the formal HIE network. Other language appears to use "health information exchange" as a *verb*, suddenly encompassing all electronic exchange of health information, whether or not through the network.

For example, in some places provisions governing "health information exchange" appear to be limited to exchange of information through some formal exchange network, often referred to by noun as a "Health Information Exchange" or HIE (or an HIO). CalPSAB's motion on uses and disclosures for health information exchange limits uses and disclosures of individual health information "through *an* electronic health information exchange" to clinical treatment and mandated public health reporting.[3] Similarly, section 2.1 of the draft Guidelines on "HIEConsent" states that an individual may opt out of having his or her information transmitted "through *an* electronic health information exchange."[4]

In other places, however, the term "health information exchange" appears to refer to any electronic sharing of data between two entities. While the motion by its terms refers to uses and disclosures "transmitt[ed] through an electronic health information exchange," the motion adds at the end that the scope of its limits on uses and disclosures for HIOs "encompasses all electronic exchanges of individual health information" and applies to "an independent [HIO], as well as to two separate health care organizations who exchange individual health information without the use of a third party organization."[5] Parts of the draft Guidelines underscore this interpretation: the term "Health Information Exchange" itself is defined throughout the draft Guidelines as "[t]he electronic movement of health-related information among organizations according to nationally recognized standards."[6]

---

[3] California Privacy and Security Advisory Board, Policy Recommendation Motions Adopted, p. 1 (Sept. 16, 2009) (italics added).

[4] California Privacy and Security Advisory Board, [Draft] Interim Privacy and Security Guidelines § 2.1.1.1 (rev. Oct. 20, 2009) (italics added).

[5] California Privacy and Security Advisory Board, Policy Recommendation Motions Adopted, p. 1 (Sept. 16, 2009).

[6] California Privacy and Security Advisory Board, [Draft] Interim Privacy and Security Guidelines § 9.0 (rev. Oct. 20, 2009) (definition of "Health Information Exchange").

As we discuss below, setting limits on all electronic exchange of information between two independent providers and allowing patients to opt out of having their information shared electronically even for purposes of clinical treatment has serious implications for quality of care.[7] We hope that the language above merely needs further clarification, and that the Advisory Board and the Secretary intend to apply the use and disclosure limits, and the opt-out policy, to exchanges through formal networks (HIOs or HIEs).

As a threshold matter, we note the perverse outcomes that could occur if the intent or effect were to limit any electronic exchange of data, whether through an HIE/HIO network or point-to-point between two discrete entities. No health data could be exchanged or disclosed electronically in any circumstance except for clinical treatment and public health purposes. Entities which today may share data legally for other delimited purposes would have to share these data in paper form for any of those authorized purposes. And in the clinical-treatment and public-health contexts, where a patient has opted out of sharing her health information electronically, sharing the patient's health information for lawfully authorized treatment purposes could only occur by paper. This does not advance meaningful use by patient or provider.

Creating constraints that apply only when data are shared electronically between providers creates an incentive for providers *not* to adopt electronic health records, because the rules governing health information exchange would be more clear—and less restrictive—for providers using all paper records. Those providers who chose to move forward with health information technology would still have to maintain a duplicate paper record in order to accommodate those patients who opted out and to perform lawfully authorized transactions with data that may not be exchanged electronically.

To the best of our knowledge, this approach is not being pursued anywhere else in the country. We are aware of states or regions that have decided to place additional constraints on how data can be accessed through a formal health information exchange network—including limiting the purposes for which the network can be used, and providing patients with an extra measure of control over whether their data may be exchanged through an HIE network (opt-in or opt-out)—but none that limit the electronic sharing of data from one physician to another for clinical treatment without the use of a formal network or third-party intermediary. New York, for example, follows existing law with respect to point-to-point exchange of health information, and the patients opt in

[7] The requirement that patients opt in for sensitive health data is of less concern (particularly if the definition of sensitive health data is limited to those conditions where patient authorization to share in any medium is required by either federal or state law) because California law already requires prior consent to share this data regardless of the medium (paper or electronic).

for network exchange.[8] The National Committee on Vital and Health Statistics, of the United States Department of Health and Human Services, adopted recommendations on consent that apply only with respect to the National Health Information Network (NHIN), not exchange of health information altogether.[9]

These adverse impacts are not justified nor balanced by any minimal gains in privacy protection that might occur by allowing the patient to opt out for *all* electronic exchanges. Consent can help to build trust, but consent alone does not constitute privacy protection, and consent alone cannot be a substitute for a comprehensive approach to privacy that actually protects patients' data and builds trust. Meaningful protection requires a balanced combination of interrelated privacy and security policies: setting and enforcing limits on data collection, use, and disclosure; ensuring patients' access to information; and providing rigorous user authentication and other appropriate mechanisms to address data security. Using a comprehensive approach to privacy means that consumer consent does not have to bear the full weight of privacy protection—which it could never do.

As noted above, the limits on the purposes for which data can be exchanged electronically and the opt-out policy (with opt-in for information requiring consent under California law) make sense if they are applied *only* to the use of a formal exchange network (exchange as a *noun*). These exchanges are new to health care, which justifies the imposition of further limits beyond what exist already in California law. If the exchange limits apply only to formal networks, the compromise advances privacy protection with a metaphoric three-legged stool: most importantly, (1) structural limits upon the allowed *uses* of a health information exchange and (2) structural prerequisites for authorized *access* to a health information exchange; and, within that strong, protective framework, (3) options for patients to opt out of having their information exchanged through a network for purposes of direct treatment (with, of course, preservation of California law requiring consent for certain types of sensitive information).

---

[8] New York eHealth Collaborative, Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State, ver. 1.1, p. 9 (Aug. 11, 2009) (available at http://www.nyehealth.org/files/File_Repository16/heal5/PrivSec_PPs_20090811.pdf).

[9] E.g., Letter from Simon P. Cohn, M.D., M.P.H., Chairman, National Committee on Vital and Health Statistics, to Michael O. Leavitt, Secretary, U.S. Department of Health and Human Services (June 22, 2006) (forwarding NCVHS's recommended actions regarding "Privacy and Confidentiality in the Nationwide Health Information Network") (available at http://www.ncvhs.hhs.gov/060622lt2.htm); Letter from Simon P. Cohn, M.D., M.P.H., Chairman, National Committee on Vital and Health Statistics, to Michael O. Leavitt, Secretary, U.S. Department of Health and Human Services (Feb. 20, 2008) (regarding "Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment") (available at http://www.ncvhs.hhs.gov/080220lt.pdf).

California's patients want privacy, but they also want the improvements in health care and the health care system that come with more widespread adoption of health information technology. We request that the Advisory Board and the Secretary correct the ambiguous language discussed above, so that the limits upon use and disclosure, and any provisions for patients to opt out of exchange for those limited uses and disclosures, apply to the formal HIE network.

Respectfully,

Mark Savage
Consumers Union of
United States

Deven McGraw
Center for Democracy
and Technology

cc: Jonah Frohlich, Deputy Secretary, Health Information Technology
Bobbie Holm, Chief, Policy Branch, Office of Health Information Integrity
Pamela Dixon, Co-Chair, California Privacy and Security Advisory Board
Rory Jaffe, Co-Chair, California Privacy and Security Advisory Board