ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

April 3, 2015

Submitted electronically
Dr. Karen DeSalvo, M.D., M.P.H., M.Sc.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue SW, Suite 729D
Washington, D.C. 20201

RE: Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap (Draft Version 1.0).

Dear Dr. DeSalvo:

Consumers Union, the policy and advocacy division of Consumer Reports, appreciates the opportunity to provide input on the Office of the National Coordinator for Health IT (ONC)'s draft *Interoperability Roadmap.* Health information technology (health IT) has a great potential for accelerating achievement of the Triple Aim of better outcomes, better quality, and lower costs. Interoperability may very well be the keystone to achieving electronic health IT that is appropriately and readily available to empower consumers, support clinical decision-making, inform population and public health, power value based payment, and advance science.

However, as eager as we are to accelerate the widespread adoption and use of health IT, we urge caution: without adequate attention to data security and patient privacy, advances in interoperability may come at a high cost to consumers and those entrusted with their health information. This letter addresses our concerns on these two aspects of the plan. Our specific feedback on the Roadmap is included in the comments submitted by the Consumer Partnership for eHealth, with which we joined as a co-signor.

Building Block #3: Privacy and security protections for health information

As a consumer advocacy organization first and foremost, we are pleased to see *Privacy and Security Protections for Health Information* listed as one of the focal "building blocks"[1] of the interoperability roadmap and commend the draft Roadmap for highlighting the risks of cyber-attacks[2]. We strongly agree with the ONC that "the success of health IT and interoperability is dependent on individuals' trust that their health information will be kept private and secure

[1] Roadmap at 55 et. seq.

[2] Draft Roadmap, pages 55-57.

Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029
(914) 378-2992 (fax)

Washington Office
1101 17th Street, NW #500
Washington, DC 20036
(202) 462-6262
(202) 265-9548 (fax)

West Coast Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 461-6747
(415) 431-0906 (fax)

South West Office
506 West 14th Street, Suite A
Austin, TX 78701
(512) 477-4431
(512) 477-8934 (fax)

and that their rights with respect to this information will be respected."[3] However, the document does not provide sufficient detail on required responses to the more likely occurrences of data breaches, both intentional and unintentional. Similar to other industries, some breaches of health information are inevitable, despite best efforts at security. The Roadmap should emphasize strategies to enforce required notice, corrective actions, and remedies for such breaches, as well as ongoing public education about the appropriate uses and exchange of personal health information to support the Triple Aim of better outcomes, better quality, and lower costs, balanced by these vital privacy and security concerns

In addition, we note that security and privacy are frequently comingled into a single concept, but they are distinct in many ways. We are therefore encouraged that this Roadmap includes the two factors as a shared building block, but also addressed as separate sub-factors. The HIPAA Security Rule, 45 C.F.R. §164, clearly distinguishes between security (§164.300 et. seq.) and privacy (§164.500 et. seq.) and addresses them separately. Security governs the "administrative, physical, and technical safeguards in an information system."[4] Privacy, on the other hand, refers to the rules that govern the circumstances under which personal information can be collected, used or disclosed. For a simple illustration of the distinction, the HIPAA Privacy Rule allows a patient's health information to be used by providers for treatment, payment and operations, but prohibits most other uses or disclosures without the express authorization of the patient. The Security Rule in turn requires health care providers to adopt certain security safeguards that reinforce or support compliance with these data sharing rules.

LHS Requirement E: Ubiquitous, secure network infrastructure

Whether consumers' privacy preferences are protected is an issue of not only recording those preferences, but also of having the technical capacity to follow-through on privacy assurances. In 2014, the FBI Cyber Division announced that "cyber actors will likely increase cyber intrusions against health care systems", and that the health care industry is "not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures … much less against more advanced persistent threats."[5] According to the same notification, nearly two-thirds of surveyed health care organizations reported a data breach in the past two years. Most recently, lapses in their data security led to a breach at Anthem, which divulged data on 80 million current and former members. In an interwoven health IT system, the failure to secure data by one organization threatens everyone.

We support the future critical actions listed by ONC in LHS Requirement E, including full encryption of network messages and data stored in databases. Of course, this standard data security precaution only works in an interoperable system if both sides of the transaction share an encryption key, which requires robust data management policies and resources to be

[3] Roadmap at 62.

[4] 45 C.F.R. §164.304 (definitions).

[5] FBI Cyber Division, Private Industry Notification, 8 April 2014. Available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

implemented successfully[6]. We leave it to technology experts to develop that protocol and urge ONC to ensure that the rush to interoperability does not mute the necessity for encryption of the maximal amount of data points. We hesitate to support selective encryption—which would certainly make encryption less burdensome—without seeing clear guidelines on what data will be left vulnerable. If the recent attack on Anthem serves as an example, unencrypted data can lead to widespread susceptibility.[7] In addition, given the speed of advances in online security threats, we urge ONC to direct technology developers, and providers using their software, to adopt a proactive approach to data security rather than one that is reactive.

Finally, we believe this Roadmap should include a framework of expectations on whose responsibility it is to respond to data breaches and the rights of consumers who are the victims of a health data breach.

LHS Requirement H: Consistent representation of authorization to access health information

Although expectations of "privacy" are arguably altered in the internet age[8], patients have long demanded and received privacy with regards to their health care. The digitization of health records—and indeed of the practice of health care in some cases—does not negate this expectation of privacy, which extends from the collection, use, and retention of electronic records to the emerging protocols of Web 3.0 and the *Internet of things*.

The need to shore up privacy rights in the digital age becomes increasingly urgent when the exchange of data becomes systematized and routine through record system interoperability. This includes both empowering consumers to designate the types of entities and persons that receive access to consumers' EHRs, and under what scenarios, as well as the ability to monitor what has accessed those records. To that end, we generally support the framework of differentiating between "basic choice" and "granular choice" in the draft Roadmap. However, we urge standardized notice to all consumers about how their personal health information will be used and shared. As ongoing health care reform activities highlight the importance of primary care and of establishing patient-centered medical homes for all patients, such notice and explanation should be incorporated into the ongoing relationship between a patient (and family and caregivers) with the primary care providers in those patient-centered medical homes.

Notably, a recent study found that the more consumers "trust that their privacy is protected, the more they use and benefit from EHRs."[9] But first, consumers need a reason to trust. In

---

[6] *Managing Patient Identity Across Data Sources* at 9.

[7] Wall Street Journal, *Health Insurer Anthem Didn't Encrypt Data in Theft*, 5 February 2015. Available at http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560.

[8] Privacy no longer a social norm, says Facebook founder, The Guardian, 10 January 2010. Available at http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

[9] National Partnership for Women & Families, *Engaging Patients and Families: How Consumers Value and Use Health IT*, December 2014, page 4. Available at http://www.nationalpartnership.org/research-library/health-care/HIT/engaging-patients-and-families.pdf.

particular, we suggest that ONC address the following key points in the final draft of this Roadmap:

1. How consumers' privacy preferences will be recorded, implemented, and retained across all care settings, and how these preferences will be applied (or rolled back) in emergency scenarios.
2. Whether patients will have the right to limit information from their digital record or have data they object to removed from the record[10].
3. Whether audit logs will build on HIPAA requirements[11] and what type of access will be granted to consumers.
4. How anonymized health records may be used for the public benefit—such as identifying health trends or disease outbreaks—while adhering to individual privacy expectations.

The lack of interoperability among much of the currently-used health IT is a broadly identified shortcoming in widespread adoption and use of developing technology for its optimal impact on health care efficiency and costs. It may also be the primary culprit behind the failure to achieve many of its anticipated advantages. Although we strongly support health IT as the foundation for achieving many of the goals set by the Affordable Care Act—and for enabling consumers to become closer partners with the providers of their health care—we also caution the ONC to develop a robust framework for securing consumers' health data and for ensuring privacy in accordance with each individual consumers' preferences.

For further information, please contact Dena Mendelsohn at dena.mendelsohn@consumer.org.

Sincerely,

DeAnn Friedholm
Director, Health Reform
Consumers Union
Policy & Action from ***Consumer Reports***
512.788.2888

[10] The European regulation, which extends to individuals the *right to erasure*, may serve as a guide for designing policy around addressing consumers' concerns about what information in stored in data that is shared across a broad spectrum of users. For more, see *Protection of individuals with regard to the processing of personal data*, European Parliament, adopted 12 March 2014. Available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

[11] HIPAA requires that, among other things, covered entities or business associates must implement information system activity review "to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 CFR §164.308(a)(1)(ii)(D).