

STATEMENT FOR THE RECORD

SUBMITTED TO THE

PCAST Report Workgroup

February 15, 2011

AARP

601 E Street, N.W.

WASHINGTON, D. C. 20049

For further information, please contact:

Joyce Dubow, AARP Office of Policy and Strategy

202-434-3901

AARP is a consumer organization representing millions of members age 50 and older. Our mission is to enhance the quality of life for all as we age, and we do this through advocacy and information. We have been an ardent and long-standing advocate for reforming the nation's delivery of health care services to assure our members and the public-at-large access to affordable, high quality care. We supported the quality provisions in the Patient Protection and Affordable Care Act of 2010 (ACA) as well as the HITECH provisions of the American Recovery and Reinvestment Act (ARRA). In our view, the combined impact of these statutes will permit significant advancements in achieving the "triple aim" of better care, more affordable care, and better health for individuals and communities.

PCAST's vision of a nationwide capability for secure exchange of health information could accelerate achievement of the triple aim by harnessing the promise of health information technology (HIT). Research evidence indicates that people recognize the value of HIT but want effective privacy and security protections in place to safeguard their information. Therefore, policymakers must assure the public their personal health information will be treated confidentially and handled in accordance with their wishes as the pace of adoption of HIT and health information exchange accelerates.

Balancing the need for data to improve care with privacy and security concerns

The Consumer Partnership for eHealth, a broad-based coalition of consumer organizations, of which AARP is a member, issued principles for HIT¹ that recognize the value of an interoperable system of electronic health information accompanied by comprehensive protections to ensure patient access and control of their personally identifiable health information. Qualitative and quantitative research supports this approach. Patients seem to be prepared to rely on HIT for many routine medical situations and want access to their complete medical records. In addition, they may value privacy less when they are sick and want their medical records available in emergency situations, to caregivers, and their clinicians.² A 2009 NPR/Kaiser Family Foundation/Harvard School of Public Health survey found most respondents believe that electronic records would improve health care delivery but also have significant concerns about the privacy of online health records. About 60 percent lacked confidence that electronic records would be able to protect the confidentiality of patients' records. And about three-quarter of respondents thought it was at least

¹ Consumer Partnership for eHealth, "Health Information Technology- Consumer Principles," 2009. Accessed on February 8, 2011 at

http://www.nationalpartnership.org/site/DocServer/Consumer_Principles- Health_IT.pdf?docID=6925

² Walker, J., Ahern, D. Lan, X, Delbanco, T., "Insights for Internists: 'I Want the Computer to Know Who I Am,'" *Journal of General Internal Medicine*, 24(6):727-32

somewhat likely that “an unauthorized person” would get access to their records if they were placed online.³

The recently released national survey of adults age 18+ conducted for the Markle Foundation found continued public (and physician) support for both online access to information and privacy protections, and also use of health information technology and health information exchange for improvement of service delivery and cost-effectiveness.⁴ Roughly 80 percent majorities of the public and doctors agree it is important to require participating hospitals and doctors to share information to better coordinate care, cut unnecessary costs, and reduce medical errors. By similar majorities, the public and doctors also agree on the importance of privacy protections as a requirement to ensure the public HIT investment will be well spent. They overwhelmingly support privacy protective practices, such as letting people know who accessed their records, breach notification, and want mechanisms to allow them to exercise choice and request corrections of their records. Finally, 68 percent of the public, and 75 percent of doctors expressed willingness to allow composite information to be used for detecting outbreaks, bio-terror attacks, fraud, and to conduct research, quality, and service improvement programs, so long as privacy safeguards are in place.

AARP appreciates the urgency expressed in the PCAST report and agrees that an ambitious agenda is needed to overcome the obstacles that deter rapid transformation of the health care system. The report presents a compelling case to take advantage of the multiple uses of electronic data—to improve health care quality and public health, help clinicians and patient make better informed decisions, conduct surveillance, and research. In doing so, it is essential that a comprehensive, workable framework for protecting privacy and data security is part of the transformation from the outset. But the PCAST report stops short of a clear articulation of a comprehensive framework, and policy recommendations to support the framework are lacking. We think the PCAST recommendations could be strengthened by including greater detail on how privacy and security concerns are fully addressed.

Do PCAST privacy and security recommendation address consumer concerns?

A comprehensive and consistent approach to address the public's concerns about privacy requires a combination of policies and technical approaches. A trust framework consisting of systems, rules, and processes that are clear and transparent to address limitations on data collection and uses;

³ NPR/Kaiser Family Foundation/Harvard School of Public Health, “The Public and Health Care Delivery System,” April 2009, accessed February 7, 2011 at <http://www.kff.org/kaiserpolls/upload/7887.pdf>

⁴ Markle Foundation, “Health in a Networked Life,” January 2011, accessed February 7, 2011, at <http://www.markle.org/health/public-opinion-surveys/latest-surveys>

individual consent and controls; oversight, accountability, enforcement, and remedies (administrative, civil and criminal) will help to reassure the public that personal health information is indeed secure. These privacy protections must be integral to the framework and embedded in its design at the outset. *Connecting For Health*, of which AARP is a member, developed policy and technical guidance for such a trust framework that consists of core privacy principles supported by sound network design, oversight and accountability.⁵ AARP supported this approach.

AARP appreciates that the PCAST report acknowledges the need for “strong, persistent privacy protections” based on fair information practices, and clear rules that are enforced about access, use, and disclosure of patient data; and also that individuals should have meaningful choices about how their personal health information is shared. However, the PCAST report relies heavily on patient consent to ensure privacy and data security, which, in our view, is not a robust protection. The additional protections we identified earlier as part of a privacy framework need to be included as well.

Will patients be able to manage the privacy controls envisioned by PCAST?

The PCAST report asserts that patients cannot make meaningful choices unless they understand the flows and uses of information. We strongly agree. Individuals need to make decisions when they have the opportunity to reflect on their choices, that is, when they are healthy and able, and have information on hand to inform their decisions. We concur with PCAST’s proposition that if people were allowed to define a finer-grained level of individual preferences they would be able to give more granular direction about, for example, whether they want their physician to see their entire medical record, past treatments, or just portions of it; whether the physician should be able to exercise discretion about sharing parts of a patient’s medical record without asking; whether medical information should be automatically synchronized to a personal health record, and the like. However, as conceptually enticing as this may be, the level of consent required to achieve the granularity envisioned by PCAST might overwhelm most patients (or their authorized representatives [e.g., family caregivers]). Can people actually manage such fine grained choices? Clearly, we already identify certain types of sensitive data (for example, mental health, HIV status, genetic information, as well as instances of domestic abuse), and there are legal protections for these data. However, we are uncertain whether the opportunity to express much greater specificity will be a welcome choice for most people.

⁵ Connecting For Health, “We Need a 21st Century Privacy Approach Allowing Americans to Protect and Share Health Information to Improve Quality”, Policy Brief, September 2008, accessed on February 8, 2011 at http://www.markle.org/sites/default/files/20080822_policy_brief.pdf

It is not clear that consumers will be able to make informed decisions about all data elements held by the multiple entities that have their data, but this is a researchable question. Importantly, patient preferences are not static and are subject to change as one's health status changes and as one ages. Therefore we need a better understanding of whether patients are able (and willing) to handle these demands. These questions need to be examined for different patient populations, among patients and family caregivers, as well as in different medical situations (e.g., acute, chronic episodes.) Research should be conducted to determine if consumers can routinely exercise the granular controls proposed for each medical occurrence and whether providers can implement the controls effectively. AARP suggests that the PCAST's recommendation should be explored and tested to determine if it is workable among different population groups and whether it can feasibly be scaled in HIT systems.

Do the data element access services (DEAS) place consumer information in a vulnerable position by establishing a single access point to query all national information?

The PCAST recommendations support a universal language based on tagged data elements and a national infrastructure for finding health data and controlling access to but not storing the data. Patients would have the right to restrict the types of data elements indexed and could opt out of the DEAS completely or selectively. AARP is concerned that the right to opt out may not be an adequate privacy protection, because most people usually do not focus or act on their right to withdraw when given the option to do so. Additional controls should be added, identifying who can access a DEAS, and for what purposes, etc.

The DEAS infrastructure would include a combination of encryption, authentication, authorization, and, for research purposes, de-identification. All patient information would be encrypted, whether stored or transmitted. Although the PCAST plan requires authentication and authorization, this is in the context of role-based access controls. The report does not identify a process for how roles would be assigned or how unauthorized access would be detected and prevented. We are concerned that the role-based authentication model still could leave patient information exposed to unauthorized use by people occupying a "legitimate" role but who nonetheless should not have access to the data.

As we understand its recommendation, PCAST would not allow the DEAS to include any patient-level health data. The Markle *Common Framework* advises against keeping any clinical information

indices on the network and against release of clinical data, even in encrypted form in order to prevent misuse by authorized individuals, therefore we are encouraged to read of PCAST's stated approach not to include such data in the DEAS. However, we have heard some doubts expressed about how this is technically possible in the PCAST scenario, given the design of the DEAS and how it is intended to function. It would be helpful to have a clearer, more detailed description of the proposed technical approach that can be understood by the lay public. We want to emphasize that we strongly believe the DEAS should not have access to clinical data and to underscore the importance of not having the patient locator service or DEAS actually be the repository of clinical data. Data should remain with the source systems and institutions. We believe it is far preferable to avoid the risks associated with a centralized repository of personal health information by means of a distributed model that leaves judgments to individual patients and their providers.

Do PCAST's technical recommendations for metadata tagging and a data element access service ensure patient choice and control, transparency, and facility adequate oversight?

The technical solutions proposed by PCAST need to be further explored and their advantages and disadvantages analyzed. The idea of tying privacy consent to pieces of data by associating patient consent to a mandatory "metadata tag" that, in turn, describes the data's attributes, where it was created, and a patient's privacy directives, seems complex and quite burdensome. Are most people willing or able to appreciate the demands of setting the privacy permissions required? ONC should pilot test potential opportunities and criteria for using metadata to determine how practical this approach is for patients and family caregivers. We need more information to understand the implications of the metadata tagged strategy. Before moving ahead with any particular technical approach to expressing privacy preferences, they should be thoroughly tested and studied.

Conclusion

AARP believes that the expanded use of HIT and HIE has enormous potential to improve clinical care, health outcomes, and public health; enhance patient engagement and activation; promote greater efficiency; and advance knowledge by facilitating research. We strongly support PCAST's vision for nationwide capability for secure information exchange using the internet; a distributed network for information sharing; use of existing identifiers to link patient information across sites; comprehensive privacy and security practices; universal exchange language for secure exchange of health information; and a focus on population health facilitated by networks of distributed health information. Achieving this important vision will require innovative and diverse solutions. We look

forward to learning more how this vision can be built on a strong foundation of privacy protections, that include not only patient consent, but also transparency, purpose specification, data minimization, use limitation, enforcement, and remedies.

ONC can play an important role in pilot testing many of the PCAST recommendations. We urge ONC to help the public understand the value of electronic sharing of information for quality and service delivery improvement by ensuring the development of a trust framework for electronic data sharing and information exchange. This means policy goals must shape technology and standards, not vice versa. We think it will be important for the ONC to reinforce approaches that keep data as close as possible to where it is captured, avoid centralized storage of clinical data, and share data only as needed. ONC could advance understanding of how data aggregation efforts within distributed models for quality reporting and improvement can be used to reach improvement goals. Finally, we encourage ONC to ensure that its work is aligned with the National Priorities and Goals and as well other efforts that promote and incent data sharing to improve care delivery.