



AARP Testimony to the Human Services Committee
March 17, 2011

S.B. 1147, AAC Patient Consent for the Exchange of Electronic Health Information

Good morning. My name is Lance Q. Johnson and, as an AARP volunteer, I am here representing nearly 600,000 members of AARP in the state. I also speak as an individual consumer excited about the many potential benefits that a Connecticut, regional, and national health information exchange (HIE) could offer to me, including: better, faster coordination of my health care; higher quality and more efficient care; increased system transparency; and access to information that would allow me to make better health care decisions. At the same time, such a system raises serious concerns among consumers about personal privacy, data security, and the potential misuse of their information. So while such a system holds great promise, the many possible benefits will not be realized unless appropriate policy measures to protect consumers are established up front.

Health information technology provisions of the American Recovery and Reinvestment Act of 2009 are providing significant federal funding to assist states and health care providers in establishing electronic medical records and health information exchange which has greatly increased the speed in which health information technology is being implemented in Connecticut. AARP CT's State Director, Brenda Kelley, is representing consumer interests on the Boards of both eHealth CT & the new Health Information Technology Exchange -- Connecticut. The pace of change is exciting. The challenge is to ensure that appropriate public policy ensuring the privacy and confidentiality of personal health information drives the design of health information exchange in Connecticut & nationally. Regulations issued under the 1996 Health Insurance Portability and Accountability Act (HIPAA) established important privacy protections for health care consumers and Connecticut also has adopted important privacy protections in state law. However, HIPAA and our state laws do not provide clear guidance in several emerging areas of electronic health care and privacy.

So AARP is pleased that the Human Services Committee is considering one important aspect of protecting consumers, **SB 1147, AAC Patient Consent for the Exchange of Electronic Health Information**. However, AARP believes that the issue of patient consent is only one of several important principles that must guide the development of public policy that protects & empowers consumers as health information technology is implemented in Connecticut and nationally.

AARP has been a leading player in the "Consumer Partnership for e Health and Health Information Technology" supported by the Markel Foundation. I'd like to share the Consumer Principles that this partnership has adopted. AARP believes these consumer principles should be reflected in state and national legislation/regulation that will protect the privacy of consumer's personal health information and will empower them to make better personal health care decisions in this new and promising age of health information technology and health information exchange.

Consumer Partnership for E Health – Consumer Principlesⁱ

Implementation of any Connecticut, regional, or national electronic health information network should be accompanied by a significant consumer education program so that people understand how the network will operate, what information will and will not be available on the network, the value of the network, its privacy

and security protections, how to participate in it, and the rights, benefits and remedies afforded to them.

Individuals should know how their personally identifiable health information may be used and who has access to it.

- Individuals should receive easily understood information identifying the types of entities with access to their personal health information and all the ways it may be used or shared.
- Access to personal health information must be limited to authorized individuals or entities.
- Tracking and audit trail systems should be in place that permit individuals to review which entities have entered, accessed, modified and/or transmitted any of their personally identifiable health information.

Individuals should have control over whether and how their personally identifiable health information is shared.

- Individuals should be able to opt out of having their personally identifiable health information – in whole or in part – shared across an electronic health information network.
- Individuals should be able to limit the extent to which their health information (with or without personal identifiers) is made available for commercial purposes.
- Individuals should be able to designate someone else, such as a family member, caregiver or legal guardian, to have access to and exercise control over how records are shared, and also should be able to rescind this designation.

Individuals should be able to access their personally identifiable health information conveniently and affordably.

- Individuals should have a means of direct, secure access to their electronic health information that does not require physician or institutional mediation.
- Individuals should have access to all electronic records pertaining to themselves (except in cases of danger to the patient or another person).
- Individuals should be able to supplement, request correction of, and share their personally identifiable health information without unreasonable fees or burdensome processes.

Systems for electronic health data exchange must protect the integrity, security, privacy and confidentiality of an individual's information.

- Personally identifiable health information should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. These safeguards must be developed at the front end and must follow the information as it is accessed or transferred.
- Individuals should be notified in a timely manner if their personally identifiable health information is subject to a security breach or privacy violation.
- Meaningful legal and financial remedies should exist to address any security breaches or privacy violations.
- Federal and state privacy standards that restrict the use and disclosure of personally identifiable health information should apply to all entities engaged in health information exchanges.

The governance and administration of electronic health information networks should be transparent, and publicly accountable.

- Independent bodies, accountable to the public, should oversee electronic health information sharing.
- Consumers should have equal footing with other stakeholders.

Consumer Partnership for eHealth, Health Information Technology – Consumer Principles, 2009

(Support from the Markle Foundation). Partners: *AARP; AFL-CIO; American Federation of State, County and Municipal Employees; American Federation of Teachers; Bazelon Center for Mental Health Law; Center for Democracy and Technology; Center for Medical Consumers; Communications Workers of America; Consumers Union; Department for Professional Employees, AFL-CIO; Childbirth Connection; Health Care for All; International Association of Machinists and Aerospace Workers; International Union, United Auto Workers; March of Dimes; Mental Health America; National Coalition for Cancer Survivorship; National Committee to Preserve Social Security and Medicare; National Consumers League; National Partnership for Women & Families; Service Employees International Union; The Children's Partnership; Title II Community AIDS National Network; United Steelworkers International Union (USW)*