# The Hon. Pete Stark, Chairman, Committee on Ways and Means, Subcommittee on Health

## Summary of Health-e Information Technology Act of 2008

## Clear Standards and Deadlines to Spur Development of Health IT Systems

Codifies the Office of the National Coordinator for Health Information Technology (ONCHIT) within the Department of Health and Human Services. This office is responsible for creating a nationwide Health IT infrastructure for the electronic exchange of health care information and facilitating the development of electronic health records that promote better quality care while protecting patient privacy.

Creates a Health IT Advisory Committee to advise and assist the National Coordinator. This Committee is made up of experts from the private sector and applicable government agencies.

In consultation with the Health IT Advisory Committee, the Office of the National Coordinator makes recommendations to the Secretary of HHS for issuing standards on three main areas: interoperability, privacy/security, and maximizing the clinical utility of Health IT.

The Secretary must finalize through rulemaking the first generation of these standards no later than September 2011.

The Office of the National Coordinator is responsible for the development of an electronic medical record system based on open source technology that meets all HHS approved technological and clinical standards. This system must be made available nine months after the first generation of Health IT standards are approved.

The Office of the National Coordinator works with the National Institutes for Standards and Technology (NIST) to test the standards and set up a system to certify Health IT systems that meet those standards.

## Incentives to Drive the Adoption of Health IT Systems

The Health-e Information Technology Act of 2008 provides needed financial incentives through the Medicare program to doctors and hospitals that adopt and use an electronic medical records system that is certified to meet standards for interoperability, security and clinical utility.

Physicians who install and utilize an approved system are eligible for incentive payments totaling up to approximately $40,000 over five years.

Hospitals that install and utilize an approved system are eligible for incentive payments of up to several million dollars.

Incentive payments for both physicians and hospitals continue for several years, but are phased out over time. Eventually, Medicare payments are reduced for those who do not use a qualified system.

The incentive policy is designed to provide time for standards to be fully developed, give providers an opportunity to plan for adoption, and reward early adopters while also providing ongoing transitional support.

The legislation also provides additional funds to help spur adoption through several grant programs. A matching grant program is aimed at providers who serve low-income areas, rural areas, and medically underserved areas, as well as non-profit facilities, and providers, such as pediatricians, who receive little or no Medicare incentives.

Additional grant programs fund low-interest loans to help providers finance Health IT systems and regional health information exchanges to unite local providers.

## Strong Rules to Protect the Privacy of Personal Health Information

The Health-e Information Technology Act of 2008 establishes a strong floor of federal privacy and security protections. It does not pre-empt any state laws or regulations that go further. The legislation:

Makes sure that measures designed to protect patient privacy do not stop at the provider's door. The legislation extends to business associates the same privacy protections and penalties that apply to doctors, hospitals and other health care providers. The legislation also expands the definition of business associate to include entities not currently covered by federal privacy laws, such as regional health exchanges.

Prohibits the sale of identifiable personal health information. Entities who hold identifiable health information must obtain authorization in order to use that data for certain purposes, such as marketing and fundraising. It also makes clear that treatment cannot be denied to anyone who refuses to provide authorization for such uses.

Safeguards the security of patient health information by encouraging the use of encryption or other methods that render patient health information undecipherable. The Act also requires that patients be notified within 60 days if a breach of their unencrypted health information has occurred.

Provides individuals the right to request an audit trail that shows any disclosure of the information held in an electronic health record.

Increases civil monetary penalties that can be levied against a health care provider or business associate for violating federal privacy rules. Gives HHS clear authority to pursue penalties for violations, even if the Department of Justice has declined to do so. Provides state Attorneys General the authority to purse penalties for violations.

It encourages accountability by requiring HHS to issue regular reports and other publications detailing when breaches of records have occurred, as well federal enforcement activities. It also, creates the position of Chief Privacy Officer to assist covered entities, business associates, and relevant federal agencies in protecting patient privacy and securing personal health information.