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

Privacy and Security Provisions of the Health-e IT Act of 2008

A strong floor of privacy and security protections
The Health-e IT 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.

Making patient consent meaningful and establishing clear boundaries on permissible uses and disclosures of patient health information
The Health-e IT Act of 2008 improves patient privacy by clarifying what uses and disclosures of health information are never allowed and making patient consent meaningful. Rather than placing the entire burden of privacy protections on patients—at times when they may be in dire need for urgent medical care and therefore least able or interested in making complicated decisions about use of their health data—the Health-e IT Act:

- creates clear rules about what types of uses and disclosures of health information are prohibited, such as the sale of health information and the unauthorized re-identification of de-identified data,
- Requires that valid authorization be sought for discretionary uses and disclosures of identifiable data like marketing and fundraising, which are not necessary for treatment, payment, or healthcare operations but which some patients may want, and
- Makes it clear that treatment cannot be conditioned on the provision of a valid authorization for these prohibited or discretionary uses and disclosures.

Holding entities accountable for safeguarding the privacy and security of health information
There are a number of entities that access, use, and maintain health information that are not directly covered by federal privacy statutes or regulations, like business associates and regional health information exchanges. The Health-e Act of 2008 holds entities that collect and maintain patient health information accountable for following the rules by:

- Expanding the definition of business associates to include entities like regional health information exchanges that did not exist at the time HIPAA was introduced,
- Applying all applicable federal privacy and security provisions to business associates, and ensuring that the penalties for violating them apply to business associates in the same manner as apply to entities already covered by federal law and regulation,
- Applying penalties to any individual or business associate that violates federal privacy and security provisions, and applying them in the same manner as currently applies only to HIPAA covered entities, and
- Allowing patients to monitor who has accessed their health information through audit trails.

Developing a culture of privacy protection through tough enforcement
To date, the Secretary has not levied a single penalty against a HIPAA covered entity, despite numerous privacy and security violations. The Health-e IT Act of 2008 encourages the development of a culture of privacy protection, both inside and outside the Department of Health and Human Services, through tough enforcement. For example, the Act:

- Increases the penalty amounts for privacy and security violations,
- Holds the Secretary accountable for actively enforcing the privacy and security provisions by requiring the Secretary to perform periodic audits, investigate all complaints for which a preliminary inquiry into the facts indicates possible willful neglect, pursue civil monetary penalties in willful neglect cases, and produce an annual compliance report that details the number and nature of complaints received from the public and how the Secretary resolved them,
- Gives the Secretary clear authority to investigate and pursue civil monetary penalties in cases where the Department of Justice declines to pursue criminal penalties, and
- Requires the Secretary to appoint a Chief Privacy Officer within the Office of the National Coordinator and to designate a privacy officer in each agency whose main responsibility will be to assist the Chief Privacy Officer in developing and implementing privacy and security policies.

Shutting down the secondary market around the sale and mining of patient data
Through these means, the Health-e Act of 2008 shuts down the secondary market that has emerged around the sale and mining of patient health information. As mentioned above, the Act prohibits the sale of health information, applies stiff penalties to any individual, business associate, or covered entity that uses or discloses health information in an unauthorized way, and requires an explicit authorization from patients before their health information can be used for marketing purposes.

Safeguarding the security of patient health information
Though the privacy of health information is important, keeping it secure is equally important. The Health-e IT Act of 2008 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 if a breach of their unencrypted health information has occurred.

Promoting privacy through the exchange of as little health information as necessary
Many health care operations can be done without identifiable health information. The Health-e IT Act of 2008:

- mandates the use and disclosure of the minimum amount of data necessary, including the use and disclosure of de-identified data to the maximum extent possible, and
- requires the Secretary to provide best practices or standards on what minimum necessary means in contexts where stakeholders might need to use identifiable health information and would like further guidance.
- directs the GAO to study the vast number of activities classified as "health care operations" and recommend which ones can be done with de-identified data or the limited data set, as defined in regulation.

The Act also requires the Secretary to review the current regulatory requirements for the de-identification of patient health information and provide guidance on how to implement them.

Privacy and security in the paper world as well as the electronic world
Finally, though the Pro(TECH)t Act of 2008 included numerous important privacy and security provisions, the Health-e Act of 2008 goes further by expanding the scope of the provisions to apply to paper records, not just electronic medical records, where applicable.