

COMPUTERWORLD

Government

Obama health care plan said to boost security, privacy controls

Privacy advocates say \$20B e-health proposal overcomes some HIPAA concerns

Jaikumar Vijayan

February 4, 2009 ([Computerworld](#)) The electronic health records plan in President [Barack Obama's \\$825 billion](#) economic stimulus bill aims to boost security and privacy controls beyond those now required under the [Health Insurance Portability and Accountability Act](#) (HIPAA).

The Health Information Technology for Economic and Clinical Health Act (HITECH) initially provides \$20 billion for the creation of a [national electronic health records](#) system that would fundamentally improve the manner in which health information is electronically created, accessed, stored, shared and controlled.

Health care security experts lauded the bill for upgrading [HIPAA controls](#) that security experts have criticized for years. Some did say they still fear that the improvements could be diluted at the request of health care lobbyists.

[Deven McGraw](#), director of the health privacy project at the [Center for Democracy and Technology](#), called the bill's proposed ban on the sale of protected health information in electronic medical records and limitations on marketing such data a key upgrade over HIPAA.

The sale and use of personal health data by health care vendors and providers has long posed a strong threat to patient privacy, according to McGraw, who on Jan. 27 testified on health care privacy issues before the [Senate Judiciary Committee](#). ([download PDF](#))

"HIPAA's provisions for when a person's personal information can be used for marketing have never been very strong," McGraw said. "It has always allowed covered entities to use patient information to send communications that have been paid for by an outside marketing company." The new proposal would require covered entities such as hospitals and physician offices to, at a minimum, obtain the consent of the patient before using his information, she said.

Another big change is the requirement that all health care providers and others using health care data disclose in a timely manner any data breach involving the unauthorized acquisition, access, use or disclosure of protected patient health information, McGraw said. The new federal rule is similar to several state laws that require the prompt disclosure of the loss of financial data.

The HITECH bill would also hold business associates -- such as billing and medical transcription services -- to the same security and privacy standards as the controllers of health care data, noted Peter MacKoul, president of HIPAA Solutions LC, a consulting firm in Sugar Land, Texas. The new bill eliminates many of the loopholes that let providers bypass similar HIPAA restrictions, he added.

The bill also calls for steeper civil fines and penalties for third parties found to be negligent in protecting health care data, MacKoul said.

McGraw noted that the [U.S. Department of Health and Human Services](#), which enforces HIPAA rules, has rarely fined health care firms for violations, despite "thousands of complaints" from patients. The HITECH bill, she said, requires that HHS imposes fines or other penalties on violators.

The proposed law also calls for HHS to more aggressively [audit health care firms](#) and their partners, and to maintain audit trails of all patient transactions. The proposed law would also require that all patient health data be encrypted.

The provisions "move HIPAA forward," McGraw said. However, she added, "We think they have been very carefully crafted, but this is not all that needed to be done." For example, HITECH doesn't allow individuals to take legal action against health care firms, she said. The legislation would let patients file complaints against providers to HHS. If the government fines a health care firm on the basis of that complaint, the individual would receive a percentage of that amount, she noted.

McGraw said the new bill's restrictions on who can access health care databases are unclear.

Deborah Peel, founder and chair of Patient Privacy Rights, a health privacy watchdog group in Austin, said the proposed privacy rules are promising, but don't go far enough in giving individuals full control of their health care data. "We believe that there should be no sharing of health care information without informed consent," she said.

While the new provisions would ban the outright sale of patient data without consent, in many cases it allows health care providers to continue sharing it with third parties, Peel said.

Peel also expressed concern that health care lobbyists may have some success in convincing legislators to water down proposed security and privacy controls, particularly those related to breach disclosure and a provision that would require health care providers to segment sensitive information at the request of a patient.