Pros And Cons Of Proposed Medicare Smart Cards

Law360, New York (January 08, 2013, 12:35 PM ET) -- On Nov. 28, 2012, the House of Representatives Energy and Commerce Committee, Subcommittee on Health held a hearing entitled “Examining Options to Combat Health Care Waste.” The Subcommittee Chairman, Rep. Joseph R. Pitts, R-Pa., stated in his opening remarks that the Centers for Medicare and Medicaid Services (CMS) must focus on “implementing mechanisms that would prevent fraudulent payments from being made in the first place” because prosecuting fraudulent providers and beneficiaries after the fact “does not get back all the money that they stole.” Thereafter, seven witnesses testified regarding new government tools to combat health care fraud.

The first witness to testify was Director of Health Care in the U.S. Government Accountability Office (GAO) Kathleen King. King shared the results of a September 2012 report on health care fraud, emphasizing that the CMS must move away from its current “pay-and-chase” model and instead focus on “effective deterrence that prevents fraud from occurring in the first place.” The remainder of her testimony and that of other witnesses addressed the GAO’s September 2012 report on health care fraud, with a particular focus on smart cards as a method of fraud prevention.

The Medicare Common Access Card Act, introduced last year in both houses of Congress, proposes that all Medicare beneficiaries be provided with a card that contains their account information. Such cards would be scanned at all beneficiaries’ health care appointments, and authorization for services would be contingent on the provider scanning the card. Providers would also be given a card, preventing fraudulent use of provider identification information.

The hope would be that such smart cards would prevent bogus providers from successfully stealing funds from the Medicare program. Bogus providers are those providers who, although they may have a national provider identification number (that is either stolen or purchased), do not provide services to real patients. Instead, bogus providers steal or purchase patient identification numbers and, using this information, bill Medicare for fraudulent services and devices.

The cards were also described as a potential tool for combatting patient-based fraud. Written testimony mentioned situations in which beneficiaries “card swapped,” allowing someone other than the beneficiary to receive medical treatment that will ultimately be paid for by Medicare. Witnesses noted that fraudulent claims can also occur when a patient provides his or her Medicare number to a provider in exchange for kickbacks.

Smart cards would verify who is eligible to give and receive benefits as a precondition to the services being provided and, in turn, the claim being presented to the CMS for payment. Each card would store the Medicare account number or identifier (today, the identifier is the beneficiary’s social security number).
Providers would also receive a new smart card that would store their National Provider Identity (NPI) number. The hope is that by requiring the identity of both beneficiaries and providers to be verified before a claim can be filed and payment processed, fraudulent claims would be prevented. The cards would also allow the CMS to adapt to one of the GAO’s recommendations: that beneficiaries’ Social Security number (SSN) be removed from their Medicare identification cards.

Representatives from two companies that provide digital security solutions testified regarding the benefits of a Medicare smart card system. Neville Pattinson, senior vice president of Gemalto Inc., submitted written testimony that stated that the implementation of such technology would “have the potential to save American taxpayers over half of the estimated $60 billion per year cost of fraud.”

Gemalto’s proposal would provide all current and new beneficiaries with a secure smart card through the mail. In a separate mailing, the beneficiary would also be provided with a personal identification number (PIN). Beneficiaries would be required to present their card and enter their PIN in order to receive medical services. The use of a smart card in combination with a PIN is known as two-factor authentication.

Providers would also receive a smart card and a unique biometric key. Requiring both parties to verify their identities and prove their presence at the time of any transaction through two-factor authentication could “[limit] the ability of criminals to fraudulently bill Medicare by posing as either a provider or beneficiary.”

Testimony from Michael H. Terzich, senior vice president of global sales and marketing at Zebra Technologies Corporation, focused on the benefit of having secured ID card printers. These secure card printers are what would prevent counterfeiting of the smart cards and are therefore imperative to the effective implementation of the proposed Smart Card system.

He noted, “even if a criminal enterprise could gain access to a secure card printer, it would still have to reverse engineer the security system, obtain secure printing supplies, hack into the secure network, encode PIN or biometric data on the smart chip, print counterfeit cards and then use those cards to create fraudulent transactions.” This is a much more challenging endeavor than merely obtaining a provider or beneficiary identification number.

Kevin Fu, an associate professor of science and engineering at the University of Massachusetts Amherst, was skeptical about the effectiveness of smart card technology as a method for preventing fraud and abuse. He warned that similar smart card systems had been successfully hacked and provided countless examples of such hacks from the U.S. Department of Defense’s common access card to France’s national health care system beneficiary card.

Fu also noted that such cards would not prevent individuals other than the beneficiary from being able to claim benefits, as the cards are not securely linked to an individual person. Fu recommended that before a large investment is made in such a system, a pilot study be performed by a neutral third party. Such a study would ideally include a security analysis and also consider the effectiveness of a smart card system as compared to other fraud-reducing tools.

The American Medical Association also submitted a letter to the subcommittee expressing concern about the considerable burden smart card implementation would place on physicians.

--By Frederick Robinson, Fulbright & Jaworski LLP
Frederick Robinson is a partner in Fulbright’s Washington, D.C., office. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2013, Portfolio Media, Inc.