STATEMENT OF PROF. KEVIN FU, PH.D.

DEPARTMENT OF
ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI
AND
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF MASSACHUSETTS AMHERST
AMHERST, MA

ON THE EXPECTATIONS OF SMART CARDS
TO REDUCE MEDICARE FRAUD

SUBMITTED TO THE
SUBCOMMITTEE ON HEALTH
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON
EXAMINING OPTIONS TO COMBAT HEALTH CARE
WASTE, FRAUD AND ABUSE

WEDNESDAY, NOVEMBER 28, 2012

Introduction

Good morning, Chairman Pitts, Ranking Member Pallone, and distinguished members of the Subcommittee. Thank you for the invitation to testify on the expectations of smart cards to combat waste, fraud and abuse in the Medicare program.

My name is Kevin Fu. I am an Associate Professor in Computer Science & Engineering with appointments at the University of Michigan and University of Massachusetts Amherst. My research investigates how to increase cybersecurity for systems ranging from smart cards to medical devices. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from M.I.T.'s Department of Electrical Engineering and Computer Science. I serve on the NIST Information Security and Privacy Advisory Board, a Federal Advisory Committee, to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in Federal Government information systems. My industrial experience in software systems includes past employment at Cisco Systems, Microsoft, Hewlett-Packard, and the Information Systems department at Holland Community Hospital.

Experiences in smart card security and health care provide me with a broad perspective on risks and benefits of deploying information security technology in health care settings:

- My cybersecurity research includes the security analysis of contactless "smart card" credit cards ("Researchers See Privacy Pitfalls in No-Swipe Credit Cards," NY Times, October 23, 2006) showing how to wirelessly lift credit card numbers, card holder names, and expiration dates from smart cards protected with the highest levels of industry standard encryption—even through wallets and clothing[1]. I have given invited talks on the benefits and risks of smart card technology at conferences, universities, companies, various Federal Reserve Banks, the Federal Trade Commission, and the Toronto Police Fraud Squad.

- I am also known for research that analyzed the security of an implantable cardiac defibrillator—demonstrating that the device could be wirelessly tricked into inducing a fatal heart rhythm ("A Heart Device Is Found Vulnerable to Hacker Attacks," NY Times, March 12, 2008)[2].

[1] http://rfid-cusp.org/

[2] http://secure-medicine.org/

- I manufacture an experimental smart card for advanced security research at universities, industrial research labs, and the Department of Defense[3].
- At a community hospital, I participated in the roll out of a smart-card precursor to authenticate health care providers for accessing paperless medical records and an electronic billing system. The less exciting part of my job involved issuing replacement authentication cards to nurses and physicians who lost their cards.

I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of HHS, NSF, or any of my past or present employers.

Smart cards

Smart cards are math in plastic. I like math. The security depends on (1) how the cards are used in a system, (2) the difficulty of breaking various algorithms, and (3) the difficulty or tampering with the physical card. A flaw in any these three elements makes a smart card vulnerable. The first element is most relevant to Medicare fraud, and is often the weakest link in the chain.

While smart cards may reduce fraud in other sectors, there remain challenges that may make deployment more costly and less effective than anticipated:

1. Smart cards authenticate smart cards, not people. For this reason, a key shortcoming of even the most perfect smart card is the difficulty of securely linking the card with a person. Linking people to a smart card is notoriously difficult.
2. There are several documented hacks against smart cards.
3. Smart card hacking will lead to increased malware on clinical computing systems.
4. Interrupting clinical workflow can lead to unanticipated consequences on patient care.

My testimony summarizes general security problems in smart cards, fraud remaining in health care programs in other countries already using smart cards, and implications for public health.

[3] http://spqr.cs.umass.edu/moo/

Problems with Smart Card and Payment Terminal Security

Below I highlight a number of security shortcomings in smart cards that led to card cloning and fraud for payments and facility access control. A common property is that the cards were seen as ironclad secure until they were not.

Chinese hack of DoD Common Access Cards. Authentication and identity systems that seem to work securely one day can lose that sense of security the next. For example, the DoD Common Access Card (CAC) was rightly cited as not having any problems with counterfeiting in 2011.

> "The Medicare Common Access Card Act of 2011 seeks to replicate the smart card technology currently used by members of our armed services and applies it to the Medicare system. The Department of Defense has issued over 20 million of these secure smart cards to authenticate and verify users for access to military programs and facilities. To date, DoD reports not a single Common Access Card has been counterfeited. We believe that seniors should benefit from the same identity security as members of our military." ("A smart approach to Medicare reform," The Hill, November 11, 2011)[4]

The DoD CAC was suggested as a model approach for the Medicare Common Access Card. Two months later, a Chinese computer virus hacked into the computers connected to smart card readers to steal PINs from DoD smart cards. The attack installed keyloggers by tricking personnel into viewing an emailed PDF file containing an exploit [5] ("New Sykipot variant can steal PINs from DoD smart cards," GCN, January 13, 2012). Security is very difficult to measure or predict; a common property of a hacked smart card system is that the smart card system was previously believed to be ironclad secure.

> "A Chinese-based cyber attack is targeting the Defense Departments Common Access Cards with technology that could steal information from military networks while troops

[4] `http://thehill.com/blogs/congress-blog/healthcare/191277-a-smart-approach-to-medicare-reform`

[5] One may wish to avoid viewing submitted testimony in a vulnerable PDF reader.

> and civilians work at their desks" ("Chinese virus targets DoD Common Access Card," ArmyTimes, January 18, 2012)[6]

Breaking into government buildings protected with smart cards. In 2006, Jonathan Westhues demonstrated the ease with which state lawmakers' smart cards for building access could be read and cloned[7]. He successfully read and cloned the ID card of California State Assembly member Fran Pavley, who remarked, "All that was done within a moment's notice of time without me even being aware of it."

Contactless credit cards hack. In 2006, I co-led a study that analyzed the security of credit cards containing contactless smart card technology[8].

> "The card companies have implied through their marketing that the data is encrypted to make sure that a digital eavesdropper cannot get any intelligible information. American Express has said its cards incorporate 128-bit encryption, and J. P. Morgan Chase has said that its cards, which it calls Blink, use the highest level of encryption allowed by the U.S. government. ... But in tests on 20 cards from Visa, MasterCard and American Express, the researchers here found that the cardholders name and other data was being transmitted without encryption and in plain text. They could skim and store the information from a card with a device the size of a couple of paperback books, which they cobbled together from readily available computer and radio components for $150." ("Researchers See Privacy Pitfalls in No-Swipe Credit Cards," NY Times, 10/23/2006)[9]

Whenever I meet a cashier with a contactless smart card reader, I ask how often customers use a contactless smart card. So far, the answer has consistently been none except for one cashier who said that the engineer who installed the reader tested a card. One cashier asked me to explain what the smart card reader did. Thus, fraud is likely low due to moderate levels of use and exposure.

[6] http://www.armytimes.com/news/2012/01/military-common-access-card-chinese-virus-011812w/

[7] http://www.yourtechtv.com/viewVideo.php?video_id=213&title=Cloning_RFID_Tags

[8] https://spqr.cs.umass.edu/publications.php?q=vulnerabilities

[9] http://www.nytimes.com/2006/10/23/business/23card.html

Chip and PIN smart card hacks. The Chip and PIN technology deployed overseas to protect credit cards is often heralded, but unfortunately this technology has also experienced several security flaws that led to fraud.

> “Cards were found to be open to a form of cloning, despite past assurances from banks that chip and PIN could not be compromised. ... For example, a physics professor...bought a meal for some people for 255 euros, and an hour and a half later, there were two withdrawals of 750 euros made from a nearby cash machine used by what appears to have been a clone of his card.” (“Chip and pin weakness exposed by Cambridge researchers,” BBC News, September 11, 2012)[10]

Many security vulnerabilities begin with complacency and a misbelief that lack of a reported security problem today means there can be no security problems tomorrow.

> “Dr Joel Brenner, the US National Counterintelligence Executive, warned that hundreds of chip and pin machines in stores and supermarkets across Europe have been tampered with to allow details of shoppers’ credit card accounts to be relayed to overseas fraudsters. These details are then used to make cash withdrawals or siphon off money from card holders’ accounts in what is one of the largest scams of its kind. ... An organised crime syndicate is suspected of having tampered with the chip and pin machines....” (“Chip and PIN scam has netted millions from British shoppers,” The Telegraph, October 10, 2008)[11]

> “The devices were modified, by adding hardware, in order to send credit card details over mobile telephone networks to the scammers.” (“Hundreds of tampered chip and PIN devices spread in stores across Europe,” Softpedia, October 14, 2008)[12]

Cloning proprietary smart cards. Many smart cards are based on proprietary algorithms that have not been tested or evaluated with strong and open peer-review. Proprietary algorithms can

[10] http://www.bbc.co.uk/news/technology-19559124

[11] http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-

[12] http://news.softpedia.com/news/Hundreds-of-Tampered-Chip-and-Pin-Devices-Spread-in-Stores-Across-Europe-95644.s

lead to a false sense of security. For instance, this Dutch researcher shows how to clone a proprietary smart card in 5 seconds on an ordinary computer with $200 in parts.

> "With more than 300 million cards sold, HID iClass is one of the most popular contactless smart cards on the market. It is widely used for access control, secure login and payment systems. ... These cards are widely used in access control of secured buildings such as The Bank of America Merrill Lynch, the International Airport of Mexico City and the United States Navy base of Pearl Harbor. ... Other applications include secure user authentication such as in the naviGO system included in Dells Latitude and Precision laptops; e-payment like in the FreedomPay and SmartCentric systems; and billing of electric vehicle charging such as in the Liberty PlugIns system. iClass has also been incorporated into the new BlackBerry phones which support Near Field Communication (NFC). ... This attack, from beginning to end runs within 5 seconds on ordinary hardware." ("Dismantling iClass and iClass Elite," by Garcia et al. 17th European Symposium on Research in Computer Security (ESORICS 2012). Lecture Notes in Computer Science, Vol. 7459, 2012. Springer Verlag)[13]

Barnes & Noble payment terminal hack. Hackers increasingly target payment terminals.

> "Hackers have stolen credit card information for customers who shopped as recently as last month at 63 Barnes & Noble stores across the country, including stores in New York City, San Diego, Miami and Chicago, according to people briefed on the investigation. ... The information was stolen by hackers who broke into the keypads in front of registers where customers swipe their credit cards and enter their personal identification numbers, or PINs." ("Credit card breach at Barnes & Noble stores," NY Times, October 23, 2012)[14]

An attack that seemed farfetched a short time ago has become real. And the attack vector may have been a modified credit card containing a virus rather than a credit card number.

[13] http://www.cs.ru.nl/˜rverdult/Dismantling_iClass_and_iClass_Elite-ESORICS_2012.pdf

[14] http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html

> “hackers installed malware on the so-called point-of-sale (POS) card readers to sniff the card data and PINs as customers typed them in. ... researchers installed their malware using a rogue credit card inserted into one device, which caused it to contact a server they controlled, from which they downloaded malware to the device.” (“Thieves hack Barnes & Noble point-of-sale terminals at 63 stores,” Wired, October 24, 2012)[15]

If a bookstore cannot protect its payment terminals from fraud, it is unlikely that a non-tech-savvy home health care worker can adequately protect a smart card reader carried from home to to car to home to use at “the point of service and use it to verify services received.”

Subway (sandwich) payment terminal hack. Demonstrating that improper use of a card technology can render a payment system insecure, Subway sandwiches suffered a massive scam dating back three years undetected.

> “a band of Romanian hackers is alleged to have stolen payment card data from the point-of-sale (POS) systems of hundreds of small businesses, including more than 150 Subway restaurant franchises and at least 50 other small retailers. And those retailers made it possible by practically leaving their cash drawers open to the Internet, letting the hackers ring up over $3 million in fraudulent charges. ... The tools used in the crime are widely available on the Internet for anyone willing to take the risks, and small businesses’ generally poor security practices and reliance on common, inexpensive software packages to run their operations makes them easy pickings for large-scale scams like this one, Marcus said.” (“How hackers gave Subway a $3 million lesson in point-of-sale security,” ArsTechnica, December 21, 2011)[16]

Stealing data wirelessly from smart card terminals. Hackers are getting more clever in how they exfiltrate data. Wireless exfiltration from a card reader is sufficiently common that Visa issued a warning to merchants.

[15] http://www.wired.com/threatlevel/2012/10/barnes-and-noble-pos-hack/

[16] http://arstechnica.com/business/2011/12/how-hackers-gave-subway-a-30-million-lesson-in-point-of-sale-security/

> "A new bulletin from Visa indicates that it is increasingly concerned about point of sale terminals being adapted to steal card data over Bluetooth connections. To combat this threat, Visa advises merchants to scan for Bluetooth signals, which could be evidence of a wireless skimming device transmitting stolen card numbers." ("Tampered card readers steal data via Bluetooth," American Banker, September 9, 2011)[17]

There is so much wireless traffic in a clinical environment, it would be extremely difficult and costly to effectively deploy wireless Bluetooth attack detectors at every smart card reader.

Subway (Boston) smart card hack. Several transit systems have suffered from hacks to the smart card payment process.

> "the students had uncovered vulnerabilities within the magnetic stripe and RFID card payment systems used for Boston Charlie Cards and Charlie Tickets. ... ("MIT Subway Hack Paper Published on the Web," PC Magazine, August 12, 2008)[18]

Dutch transit smart card hack. The Netherlands is home to several companies in the smart card industry. Unfortunately, the smart card system for transit payments was hacked.

> "The Dutch RFID public transit card, which has already cost the government $2B — no, that's not a typo — has been hacked even before it has been deployed. ... My guess is the system was designed by people who don't understand security, and therefore thought it was easy." ("Schneier on Security: Dutch RFID Transit Card Hacked," Schneier blog, January 21, 2008[19])

International Problems with Smart Cards in National Health Programs

A number of countries already use smart cards for national health programs. One of the more interesting uses is to store a mini electronic health record on each card so that providers have in-

[17] http://www.americanbanker.com/security-watch/bluetooth-skimming-1042020-1.html

[18] http://www.pcmag.com/article2/0,2817,2327898,00.asp

[19] http://www.schneier.com/blog/archives/2008/01/dutch_rfid_tran.html

stant access to prescription data in emergencies and patients receive more consistent care across different providers ("Health care abroad: Taiwan," NY Times, November 3, 2009). Unfortunately, national health programs relying on smart cards for authentication continue to suffer from fraud and abuse. The articles below illustrate the types of problems one should not expect smart cards to solve in the Medicare program.

France: Fraud and photographs. In France, the "carte vitale" smart card has been in place since 1998. Until 2007, beneficiary cards did not include a photo[20]; it was routine for people to use other people's cards. In the French system, many health care professionals still do not have the smart card readers after nearly 15 years. In such cases, a patient pays the provider directly and instead uses an ancient paper-based system for reimbursement. Thus, loop holes persist for fraud. The French must maintain two separate payment processing systems.

> "Why launch a new version of the card? ... It is also open to fraudulent use." ("French carte Vitale to be upgraded," FrenchEntrée, 2006) [21]

A common source of smart card fraud happens during the vulnerable registration process. A secure smart card is much less effective against fraud if registration process remains weak.

> "Inadequate checks by social security authorities leave the system open to abuse by foreigners..." ("Calls to tackle carte Vitale fraud," The Connexion, May 5, 2009) [22]

> "Even if identity documents are becoming more and more secure...the requirements for obtaining these documents are particularly lax. ... it is easy to get a birth certificate for a borrowed identity or to counterfeit an identity. ... the carte Vitale is the object of massive fraud and there is no serious securitization process in place." ("France faces rise in identity fraud," Le Figaro, November 14, 2011) [23]

[20] N.B.: the proposed legislation in H.R. 2925 would also not include photos on beneficiary smart cards. However, including photos for the Medicare beneficiary demographic would likely prove infeasible to implement.

[21] http://www.frenchentree.com/france-lot-quercy-services-contacts/DisplayArticle.asp?ID=18469

[22] http://www.connexionfrance.com/news_articles.php?id=797

[23] http://plus.lefigaro.fr/note/france-faces-rise-in-identity-fraud-20111114-598540

> “The cards can also be used fraudulently, with the consent of the owner. Attempt to limit the phenomenon, all new cards issued Vitale since 2007 (about 15 million copies) include a photo. But the effectiveness of the measure - which apparently has never been evaluated - remains to be seen.” (“Vitale card biometric expensive and difficult to implement,” translated from Le Figaro, August 3, 2012)[24]

Taiwan: Provider fraud and collusion. The Taiwanese Bureau of National Health Insurance deployed a smart card system several years ago. While there are few reports of card cloning, more serious fraud persists because of collusion between patients and providers.

> “surgeons from the Taitung Hospital...fabricated medical records to claim subsidies from a Ministry of Health program to subsidize outpatient and inpatient service for intern physicians. ... supervisors...filed false medical record entries ... had also fabricated the visits of 36 patents” (“Prosecutors charge one surgeon, defer another in health insurance fraud case,” The China Post, September 9, 2009)[25]

According to a security expert in Taiwan, multiple patients collude with one or more doctors to report higher examination and medication fees to the insurance payment system supervised by Bureau of National Health Insurance, such that they can split the extra money among themselves.

> “a former gynecologist ... allegedly performed surgeries on healthy patients, claiming more than NT$500,000 in reimbursements from the Bureau of National Health Insurance. He also gave patients chemotherapy to help them obtain tens of millions of dollars in insurance payouts.” (“DOH to clamp down on health insurance fraud,” Taipei Times, March 29, 2010)[26]

Even a secure smart card cannot stop this kind of fraud.

[24] http://www.lefigaro.fr/conjoncture/2012/03/08/20002-20120308ARTFIG00545-fraude-a-la-secu-sarkozy-veut-une-carte-vitale-biometrique.php

[25] http://www.chinapost.com.tw/taiwan/local/taitung/2009/09/09/223867/Prosecutors-charge.htm

[26] http://www.taipeitimes.com/News/taiwan/archives/2010/05/29/2003474144

Germany: Fraud and ballooning costs. After years of delay, Germany has spent its first billion of investment funds to issue smart cards (called Gesundheit) for its national health program ("Resistance to electronic health card: we do not have photos for you," translated from Süddeutsche.de, August 17, 2012).

> "The fraudulent misuse of health insurance cards caused billions in damage. ... The principle of the card cheater is easy: either several non-insured use a smart card together...or a group of relatives and friends in Germany. Sometimes the cards were also stolen from a deceased of those insured who have changed their policies, but have not yet returned the card." ("Smart card: Rip-offs by medical card," translated from Frankfurter Allgemeine, January 13, 2004)[27]

The deployment proved difficult when the smart cards were accidentally distributed without PINs.

> "Embarrassing mishap of the electronic health card: approximately two million patients have received faulty payment cards. The manufacturer promises to replace the defective copies quickly." ("Breakdown: Millions of faulty health payment cards," translated from Der SpiegelOnline, June 22, 2012)[28]

UK: Providers sharing smart cards. The British have discovered that general practitioners share their National Health Service smart cards.

> "A recent survey conducted by the GP's newspaper Pulse revealed that one in six NHS staff flouted the rules regarding confidential medical records, and shared smartcards. Despite CfH warnings that 'disciplinary procedures should follow' if smartcards are used improperly, 5% of GPs also admitted sharing their own smartcard." ("NHS loses contact to smartcards," Smartcard & Identity News, December 2008)[29]

[27] http://www.faz.net/aktuell/gesellschaft/kriminalitaet/chipkarten-abzocken-per-krankenkarte-1147791.html

[28] http://www.spiegel.de/wirtschaft/service/kassen-verschicken-elektronische-gesundheitskarten-ohne-pin-a-840405.html

[29] http://www.smartcard.co.uk/articles/NHSLosesContact.php

Australia: Terminating smart card contract. Australia is beginning to deploy smart cards for their national health program, but has run into snags in the USD$ 25M system.

> "IBM's AU$23.6 million contract with the National E-Health Transition Authority (NEHTA) is in tatters, and both sides have brought the lawyers in as the government implements an interim National Authentication Service for Health (NASH) system. ... IBM was tasked to develop a system that would use public key infrastructure and secure tokens, such as smart cards, in order to provide an authenticated service." ("Legal woes for IBM's e-health contract," ZDNet, October 25, 2012)[30]

Implications for Public Health

The overly trusting beneficiary. My understanding is that a significant source of fraud comes from home health care services. A home health care patient who cannot remember to eat breakfast on his own is not going to be able to remember a PIN or password. A patient who qualifies for home health care can literally be home-bound. For instance, the patient might not be able to independently shop for groceries for over a year. A stroke victim who must relearn how to swallow may not be able to talk or feed herself without assistance. Thus, a home health care patient depends greatly on the kindness of others, and can be particularly vulnerable to overly trusting a provider. A vulnerable home care patient would likely comply with an unscrupulous provider who asks to "hold on to the smart card and PIN so as not to inconvenience the patient." In short, smart cards that work well for the subway traveller or retail shopper will likely not work as effectively for the demographic of home health care.

Malware on clinical computing systems. Because payment software for smart card readers are prone to targeted malware, requiring this software installed will increase the exposure of clinical computing systems to malware. How many systems will be exposed to malware? Over 1,058,469 Medicare physicians/suppliers billed Medicare last year.

[30] http://www.zdnet.com/au/legal-woes-for-ibms-e-health-contract-7000006359/

> “Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable. ... malware at one point slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards.” (“Computer Viruses are Rampant on Medical Devices in Hospitals,” MIT Technology Review, October 17, 2012)[31]

All hospitals struggle with reducing the amount of malware reaching their critical care systems. The malware often spreads via webmail accounts, networks—and USB sticks that circumvent all firewall controls. Medical device manufacturers often disallow the use of anti-virus products. Thus, clinical computing systems can suffer from severe consequences when infected with malware. Downtime can lead to delayed patient care (e.g., transporting seriously ill patients waiting for a time-critical angioplasty from a cath lab infected with malware that renders the surgical equipment unavailable) to faulty sensor readings. A cath lab is one USB stick away from a terminal connected to a smart card reader.

Because malware has spread from a chip and PIN smart card to the payment terminal, health care computing systems will likely become more vulnerable to malware that can steal or tamper with medical information.

Questions

There are several questions on smart cards for Medicare that require more thought to find a meaningful answer.

1. Given that beneficiaries already share their paper cards, what would disincentivize these same beneficiaries from sharing a smart card and PIN?
2. How likely would a patient over 65 forget a smart card, give the smart card to a friend, or write the PIN on a sticky note and let a home health care provider hold on to the smart card?

[31] http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

3. What is the clinical impact of introducing extra procedures to the critical path of the delivery of patient care if the card must be scanned “at the point of service and use it to verify services received by placing into a reader, entering their PIN, and confirming the transaction”? One of the greatest sources of medical errors leading to patient harm is a complicated clinical workflow. There could be benefits or risks, but the answer is unknown.

4. Who pays for the materials and time spent by health care professionals when a smart card vulnerability necessitates a reissuing of smart cards or smart card readers before the anticipated replacement date? What business will legitimate providers lose if the billing systems are unavailable or reverted to paper?

5. Who is responsible if a patient is harmed by malware spread to the clinical environment as a result of vulnerabilities in payment process software that connects to each smart card reader?

6. Who guards the guards? How bribable are the guards? When a smart card is lost, who has the authority to replace the card? In the case of the hospital where I worked, I had the authority to issue new cards to health care professionals. My salary at the time amounted to approximately $1\frac{1}{2}$ large pizzas per day.

Recommendations

The expected benefits of smart cards need to take into account the full costs and risks shouldered by the non-fraudulent providers and beneficiaries. I would recommend the following:

1. A pilot study should include a security analysis and penetration testing of the system by a neutral third party, as well as tests designed with clinical engineers and health IT specialists to measure the impact on patient care.

2. A pilot study should measure fraud in comparison with alternatives. For example, it would be useful to know to what extent a less expensive photo ID would reduce fraud compared with

a smart card because other countries are increasingly adding photos to beneficiary cards to curb fraud[32].

3. A smart card pilot should measure the impact on fraud while controlling for fraud reductions due to fraud detection systems and strengthening of provider enrollment. That is, the smart card benefits should not be conflated with the benefits from other fraud reduction mechanisms.

4. There should be a period of public feedback coordinated by a neutral third party who has no financial interest in the outcome of the selected technology. NIST may be a logical choice given that the proposed legislation refers to NIST standards.

Conclusion

It is important to reduce fraud, waste and abuse in the Medicare program. Given finite resources, does it make sense to invest in smart card infrastructure rather than better fraud detection systems? Rather than strengthening of provider enrollment? These questions are worth exploring, but the proposed pilot program does not explore such questions. Moreover, a pilot ought to account for the costs of time that health care professionals must spend to coordinate two separate billing systems (the smart card and the paper backup) rather than delivering care, especially in home health care and durables—two segments known for significant fraud. If the pilot program were redesigned for a comparative analysis between different fraud reduction approaches, one could better determine which approaches have the best return on investment.

A key lesson from modern cybersecurity research is that security technology alone will not solve a security problem unless there is effective policy implemented to control fraud. Without first plugging the policy loopholes that lead to Medicare fraud, the Federal Government will likely switch from maintaining one costly, fraud-prone system to instead maintaining two costly, fraud-prone systems.

Thank you. I am happy to answer any questions you may have.

[32] However, obtaining photos for the Medicare beneficiary demographic may prove challenging.