Testimony of
Neville Pattinson
Senior Vice President
Gemalto, Inc.

On behalf of the
Secure ID Coalition

Before the
House Energy & Commerce Subcommittee on Health

Hearing on
Examining Options to Combat Health Care Waste, Fraud, and Abuse

November 28, 2012

919 18th Street, NW, Suite 925 | Washington, DC 20006 | p: 202.464.4000

TABLE OF CONTENTS

About the Secure ID Coalition:
Founded in 2005, the Secure ID Coalition works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections we advocate for technology solutions that enable individuals to make decision about the use of their own personal information. Members of the Secure ID Coalition subscribe to principles that include the increased deployment of secure identity solutions, as well as advise on and advocate for strong consumer privacy protections and enhanced security to reduce waste, fraud, theft and abuse. Our mission is to promote the understanding and appropriate use of smart card technology to achieve enhanced security for ID management systems while maintaining user privacy. Such ID management systems include physical and/or logical access to facilities and networks. For more information, please visit our website at www.secureIDcoalition.org.

INTRODUCTION

Thank you Chairman Pitts, Ranking Member Pallone, and Members of the Subcommittee for inviting me to testify on solutions to the problem of Medicare fraud, waste and abuse. My name is Neville Pattinson, Senior Vice President, Gemalto, and I am here today representing the Secure ID Coalition.

Gemalto is the world leader in digital security with North American headquarters in Austin, TX and 2011 annual revenues of over $2.5 billion. With over 10,000 employees operating out of 74 offices and 14 Research & Development centers, we are dedicated to delivering innovative products, services, and solutions for our customers in over 40 countries. Gemalto issues more than 1.2 billion credentials per year out of our 18 production and 30 central issuance centers, which are certified to the highest security standards in the industry. To find out more about us please visit www.gemalto.com , blog.gemalto.com, or follow us on Twitter: @gemalto_NA.

Founded in 2005, the **Secure ID Coalition** is composed of companies which make smart cards and their attendant technologies. We work with industry experts, public policy officials, and federal and state agencies to promote identity policy solutions that enable both security and privacy protections.

We are here to offer our industry expertise in the area of smart cards, which are used extensively throughout the federal government and around the world to protect access to both physical and logical assets, as well as to protect personal information.

IMPROVING MEDICARE & MEDICAID PROGRAM INTEGRITY

Prevention is 90 Percent of the Cure

Our nation's Medicare and Medicaid programs are under attack. The Centers for Medicare and Medicaid Services (CMS) estimated that in 2010, over $65 billion dollars in improper federal payments were made through both the Medicare and Medicaid programs. An April 2012 study published in the Journal of the American Medical Association estimated that fraud and abuse cost Medicare and Medicaid as much as $98 billion dollars in 2011.[1] Despite these good faith estimates, the true cost of fraud and abuse in health care remains unknown; however one point is certain: the financial impact of waste, fraud and abuse threatens the very existence of the Medicare and Medicaid programs.

The reason for such a monumental waste of taxpayer funds is a systemic lack of accountability: criminals posing as durable medical equipment providers billing Medicare for products never

[1] Berwick, Donald M. and Andrew D. Hackbarth, "Eliminating Waste in US Health Care," *JAMA* 307, no. 14 (2012): 1513–6, doi:10.1001/jama.2012.362.

sold, rogue providers billing for services never rendered, and inattentive office staff billing Medicare for treatments never allowed. If fraud, waste and abuse within the Medicare and Medicaid systems are ever to be curbed, the very first place we need to start is being able to know and verify who is authorized to provide and receive these important benefits – while preventing those who are not – before the claim is ever made.

Unfortunately, our current inability to address this fundamental identity and verification problem leaves both the Medicare and Medicaid systems perpetually open to ongoing exploitation. Programs to curb Medicare and Medicaid fraud, waste and abuse without first resolving the identity verification problem will ultimately fail if we don't know who is a legitimate beneficiary or provider, and who is not.

Structuring the Medicare and Medicaid systems to prevent fraud will not only save taxpayers billions of dollars every year, but ensure that these two very important programs survive to serve Americans now and well into the future.

Securing the Cards and Transactions

Our recommendation is to address the problem of **identity verification** of beneficiaries, providers and suppliers as well as **securing billing transactions** in Medicare. The proposal calls for upgrading the Medicare card to secure transactions as has been done in other federal programs and other health programs across the world. Many or our recommendations are contained in the **Medicare Common Access Card Act** introduced last year in the both the House (HR.2925) and Senate (S.1551), both of which are endorsed by the American Association of Retired Persons (AARP). These bills call for an upgraded Medicare card, based on a secure smart card, to verify who is eligible to give and receive benefits as a pre-condition to the claim ever being presented to the Centers for Medicare and Medicaid Services (CMS) for payment.

Under the proposal for beneficiaries, the new smart card would securely store the Medicare account number or identifier (which today is the Social Security number) on a secure micro-controller. Providers and suppliers will also receive a new smart card, securely storing their National Provider Identity number (NPI), so that only they can use it. By requiring identity verification of providers and beneficiaries before a claim can be filed and payment processed, Medicare would easily eliminate more than fifty percent of the fraud within the current system. Smart card solutions are used throughout the Federal government as employee credentials, within the States as benefits cards, and in local hospitals and health systems to reduce errors, eliminate duplicate electronic records and to save administrative costs. For the purposes of this bill, the program outlined calls out Medicare specifically. Our industry has been discussing and promoting an upgraded Medicare card to reduce fraud, waste and abuse within the program over the past several years.

However, smart cards could easily be deployed within Medicaid. Currently, several states including Georgia, North Carolina and Virginia are considering smart cards and biometrics

programs as a way to reduce fraud, waste and abuse within Medicaid. The Secure ID Coalition continues to reach-out and dialogue with a number of healthcare providers and others in the healthcare community to educate them about the potential benefits of the smart card technology solution.

WHAT IS THE PROBLEM?

Provider-Based Fraud and Error:

- Phantom billing is where fraudsters or unscrupulous medical providers bill Medicare for unnecessary or unperformed procedures, medical tests, or equipment (or for equipment that is billed as new but is, in fact, used).

- NPI numbers of upstanding providers are stolen by fraudsters and criminals and used to file claims. In this case providers are unaware their Medicare account is being used for nefarious purposes.

- Durable medical equipment abuse can happen when medical equipment used in the home - like wheelchairs or oxygen tanks - are billed many times over, while in fact nothing has been delivered to an actual patient.

- Processing errors and mistakes account, in many cases, for improper payment. These payments either should not have been made or were made in an incorrect amount. Improper payments also include payments sent to the wrong recipient or payments where supporting documentation is not available.

Patient-Based Fraud:

- Fraudulent patient billing can occur when a patient provides his or her Medicare number to a provider in exchange for kickbacks. The provider bills Medicare for any reason and the patient is told to admit that he or she indeed received the medical treatment.

- "Card Swapping" passed-off or stolen Medicare cards are used by others to get medical care.

WHAT IS THE SOLUTION?

A Medicare Common Access Card

The term "common access card" derives from the original federal government smart card program: The Department of Defense's Common Access Card (CAC). The DOD CAC was implemented in 2000 as a means of authenticating personnel with access to DOD facilities and computers. Upon full deployment, network intrusions were reduced by nearly 50% overnight. The CAC model and platform has also been rolled out across the federal government for all employees and contractors known as the Personal Identity Verification (PIV) program.

A Medicare CAC would leverage the existing government platform for secure identity credentials to modernize how information is protected within the Medicare system itself. Doing so protects the personal information of every beneficiary and puts in place a front-end prevention system to only allow authorized providers and suppliers to bill for Medicare services.

Authenticating Medicare beneficiaries and providers during an enrollment process and requiring the use of secure personalized credentials will reduce fraud by:

- Verifying beneficiaries are authorized to receive services and pharmaceuticals or equipment being prescribed;
- Verifying providers are authorized to provide those services and bill Medicare;
- Verifying suppliers, such as durable medical equipment (DME) vendors, are authorized to provide products and/or services and bill Medicare
- Preventing imposters from posing as beneficiaries or providers, thereby thwarting fraudulent transactions; and
- Verifying and coding each transaction to prevent phantom billing, processing errors and DME abuse.

Further, an upgraded Medicare card would protect beneficiary's privacy by taking their Social Security number off the front of the Medicare card, and locking it securely within the card's onboard computer chip – an important step in helping to reign in identity theft.

Card Issuance and Use

Today when a beneficiary first enrolls in the Medicare program they verify their identity with documents or certificates on record with the Social Security Administration. Under Medicare CAC the process for beneficiary enrollment would not change. After electing to receive Medicare, beneficiaries receive a new secure smart card in the mail containing their protected identification information on an embedded micro-controller. For security purposes, a unique PIN code would be mailed to the beneficiary separately. The card and PIN together authenticate the beneficiary at check-in and authorize the transaction with the provider at the point of service or check-out. This process, using a smart card with a PIN code, is known as two-factor authentication.

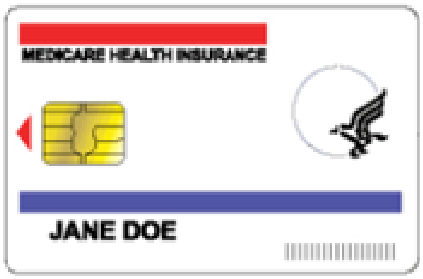
Medicare providers verify their identity and eligibility to provide services during an enrollment process. Currently, under the Affordable Card Act (ACA) high risk providers go through an enrollment process to verify their credentials and identity. Under the proposed Medicare CAC, each provider's identity is secured by supplying a biometric that will serve as their own unique key to their Medicare billing account. Providers receive a secure smart card which includes an embedded micro-processor that stores basic biographical information, their NPI, as well as their unique biometric key, thus binding the credential to the individual. The card and the biometric together authenticate the provider, similar to two keys used to open a safety deposit box (another type of two-factor authentication).

At the point of service, the transaction is authorized by both the provider and the beneficiary by creating an electronic verification between their two smart cards using the unique keys – in this case, the beneficiary's PIN code and the provider's biometric. This verification is critical as it creates a confirmation by both parties that the service was rendered. The two-factor authentication process (card plus PIN for beneficiaries and card plus biometric for providers) limits the ability of criminals to fraudulently bill Medicare by posing as a either a provider or beneficiary. It's important to note that this represents two major improvements over the current system: first, a successful transaction requires two parties, and second, each of those parties must provide two-factor authentication of their respective identities.

(Continued next page)

How Medicare CAC works in the doctor's office

Provider Credential



Beneficiary Credential

Both the Medicare Provider and the Beneficiary will be issued Medicare Common Access Card type credentials. The Provider's credential will have a name, photo ID, and a computer chip containing the provider's biographical information, National Provider Identity (NPI) number and their unique biometric key, all securely encrypted. The Beneficiary's card will only have the Beneficiary's name and the secure encrypted computer chip, which contains relevant biographical information, and their Social Security number, which is also their Medicare account number. No longer will a beneficiary's SSN be printed on the front of the card, further protecting the Beneficiary's personal information and privacy.

When checking out, both the Beneficiary and the Provider simultaneously insert their cards into the card reader. This ensures that both parties are present to verify and approve the transaction prior to billing CMS.

In order to actually process the transaction, the Beneficiary inputs their secret PIN number and the Provider scans their fingerprint biometric, verifying that both parties are who they say they are, and both agree to the transaction.

Click here to visit the Secure ID Coalition's website and see a video of the process in action.

HOW WILL MEDICARE CAC SOLVE THE PROBLEM?

Authenticating Identity of Beneficiaries, Providers and Suppliers

Unauthorized services and product transactions are essentially eliminated since both the secure smart card and the person who owns the key on the card are required to conduct the transaction. This means that phantom billing, fraudulent patient billing and stolen Medicare cards are no longer easy means of bilking Medicare. Furthermore, both parties to the intended transaction must verify the transaction. In addition to imposing strict anti-fraud mechanisms, a Medicare common access card would also reduce processing errors (duplicate or misdirected payments) through electronic verification of data and digitally signed electronic billing processes.

The Proposed Medicare Common Access Card does not call for use of biometrics for beneficiary authentication.

As discussed above, the proposal calls for patients to authenticate their identity via the Medicare CAC smart card and a unique PIN. Within the healthcare industry, biometrics are increasingly used for identification due to concerns about patient safety, identity theft, and insurance fraud.

While biometrics are among the most accurate identity verifiers, and are currently used to identify people in many diverse settings including amusement parks, airports, public schools, hospitals, retail outlets and federal government facilities, we are not recommending biometrics for Medicare or Medicaid beneficiaries at this time due to the significant challenges and costs of enrollment.

Authentication of Medicare Providers and Suppliers

Biometric authentication is recommended, however, for providers and suppliers in the Medicare CAC system. This would extend to billing agents within a doctor's office or hospital.

Biometrics is the science of identifying people based on certain unique physical characteristics. Examples of types of biometric identification include facial geometry, fingerprint, hand, retina and iris. As part of Medicare CAC, and in a secure smart card environment, biometric data is distilled to a mathematical calculation known as a *template*. Because the template is a representation of the biometric and not the actual image, it cannot be reproduced, copied or stolen. The biometric template is encrypted and securely stored inside the micro-controller embedded in the provider's smart card. At the point of verification, the card is placed in a card reader. No information on that card can be read until the biometric that was provided at enrollment is presented and read. The smart card and the reader would then perform a *one-to-one match* (also known as *match-on-card*) between the template on the card and the live

image. The biometric is confirmation that the person to whom the card belongs is present. Because no one would have the associated biometric except for the rightful individual, the system prevents fraudulent behavior. As a result, CMS is afforded the ability to use biometric authentication without maintaining an online national biometric database.

Some biometric systems require an online database to which images are matched when they are presented for verification. This process is called a *one-to-many match*. In the case of Medicare this approach is not recommended because there is no need to try to determine who is filing the claim, only a need to verify that the claim is being filed by the person authorized and to whom the card was issued. The one-to-many match requires constant online access to a central Medicare biometric database and is used to answer the "who is this" question. It would require providers to wait for verification of a one-to-many match process which can take significant time. Having a central Medicare biometric database accessible online is also an invitation for hackers and fraudsters to attempt to breach the system. A one-to-one or match-on-card system answers the "is the person I think it is" question of concern.

For a secure, authenticated Medicare system, a one-to-one match using biometric templates is the recommended approach, giving each provider complete control over their card and verification process. Making authentication easy and less time-consuming benefits both beneficiaries and providers.

Medicare Beneficiary Privacy and Security

A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways. First, the beneficiary's Social Security number (SSN), used today as the Medicare Claim Number, will no longer be printed on the card and readily available to identity thieves. The identification information is encrypted and stored safely on the secure embedded chip. Second, information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code. Third, personal information is protected through encryption when transmitted electronically and when stored. The Medicare Common Access Card not only improves the patient's privacy and security in a medical environment, but it strengthens the beneficiary's overall privacy, reducing opportunities for identity theft and fraud.

Medicare Provider Privacy and Security

The secure Medicare smart card system similarly protects the privacy and security of the provider's information. NPI's and other personal information will no longer be printed on the front of the card; instead, it will be encoded on the card's secure embedded chip. As with beneficiaries, only an authorized Medicare card reader system can access the information on the card, and then only when the provider has consented to present his biometric. These precautions not only protect the legal card holder's privacy, but also ensure the integrity of the

system from fraudsters who steal a provider's card in order to make an unauthorized transaction.

Realizing that providers don't always file the claim to Medicare themselves, the Medicare CAC offers flexibility in that administrative personnel can also be equipped with a Medicare CAC card as an authorized representative of the provider after undergoing the same enrollment process as the provider. To file the claim, the provider's NPI would be securely stored on the authorized representative's smart card. This flexibility alleviates the need for providers to be present to file a claim, and presents no interruption in provider workflow.

Common Access Card: NIST Approved Open Standards

In the U.S., open standards for secure identity credentials such as the DOD CAC and PIV cards were developed collaboratively by industry standards organizations with the participation of the U.S. government through the National Institute for Standards and Technology (NIST). The NIST standards were jointly developed to protect both physical and logical (computer networks) government infrastructure against attack.

The Office of Management and Budget, through OMB M-11-11, mandated that every federal agency, including the Department of Defense, utilize secure smart cards to authenticate and verify users for building access and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cyber security attacks on the first day of secured logical access implementations in any given department. The U.S. e-Passport is based on the same underlying secure identification technology and was implemented to prevent unauthorized access into the United States.

WHAT ARE THE BENEFITS OF A MEDICARE SMART CARD TO BENEFICIARIES, PROVIDERS AND TAXPAYERS?

Benefits to Beneficiaries
A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways.

- **Social Security Number Removed From Front of Medicare Card**
  The beneficiary's Social Security number (SSN) is no longer printed on the card and readily available to identity thieves. The identification information will be stored safely on the secure embedded chip.
- **Beneficiary Consent**
  Information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code.

- **Personal Information is Encrypted**
  Personal information is protected through encryption when transmitted electronically and when stored.
- **More Funds Available for Legitimate Care**
  Reduction in fraud within the system makes more funds available for legitimate healthcare needs of Medicare beneficiaries.

Benefits to Providers and Suppliers
A secure Medicare smart card strengthens providers' privacy and security in a number of ways and enables more efficient business practices.

- **Quicker Processing of Payment**
  Because transactions are verified by both the provider and beneficiary a non-repeatable audit trail is created. This electronic processing eliminates paperwork and streamlines to payment cycle, allowing for quicker and more accurate payment to providers.
- **Billing Accuracy**
  In many cases claims are rejected because of small mistakes or typos. Because the chips verify both the provider and beneficiary all information is electronic, eliminating these types of mistakes.
- **Reduces Need for Recovery Audit Contractors**
  Because both beneficiaries and providers provide proof they are legitimate, payment is pre-approved before it is sent, reducing the need for backend recovery audit contractors.
- **Streamlined Processes Increase Administrative Efficiency**
  Smart cards store basic patient and beneficiary information on the secure chip. That information can be accessed by the provider at point of check-in to identify the correct patient record and eliminate many of the administrative check-in procedures.
- **Protects Medicare Provider Numbers**
  Today provider numbers are widely available and used by thieves billing Medicare for products and services never performed. Using a smart card guarantees that no one can masquerade as the provider and use their number to bill Medicare.
- **Traceability/Audit trail**
  Using a smart card as part of the billing process creates an unrepeatable audit trail definitively verifying the details of each transaction between beneficiary and provider. Since the information is electronically signed and transmitted to CMS processing the information cannot be changed, altered or hacked.

Benefits to Taxpayers
While both beneficiaries and providers receive protections and benefits within the system, taxpayers ultimately gain the most significant benefit: reduction of fraud, waste and abuse within the Medicare system. Taxpayer funds can now be targeted directly to those Americans entitled to Medicare benefits, without fear of siphoning by crooks. Such a program will go a

long way towards providing stability and restoring integrity in a program on which so many Americans rely.

WHERE HAS THIS TYPE OF PROGRAM BEEN SUCCESSFUL?

Smart cards are used in the US and around the world to prevent fraud and reduce costs. Below are just a few examples of smart card deployment that have resulted in significant savings.

US Healthcare

While there are myriad examples of smart card implementations in healthcare across the US, we've chosen to highlight two showing cost savings for both large and small hospitals alike.

- Mt. Sinai Hospital, New York City. When Mt. Sinai deployed smart cards to their patients to reduce the number of duplicate or overlaid records in their system, estimated to be close to 15%. The hospital was able to eliminate annual large scale medical record clean-ups which cost the institution $1.8 million and involved over 250,000 duplicate records. Additional benefits included the elimination of the patient clipboard paperwork and reduction in medical errors.

- Memorial Hospital, North Conway, New Hampshire. Memorial Hospital reduced admission errors from 6% of patient records to less than 1% by deploying smart cards, including the reduction of medical record error from a rate of 7% to less than 1%, creating an annual savings of $55,000 for a 35 bed hospital. Patients saw a direct benefit as Memorial Hospital was able to reduce their admission time from 22 minutes to less than 3 minutes – an immediate cost savings of $574,000 in annual employee payroll minutes, which allowed Memorial to redirect staff to other productive tasks.

International Healthcare

A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

- French healthcare system SESAM-Vitale. The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.

- German Ministry of Health. Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800

million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

- Taiwan. The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

Financial Services

The smart card technology present in the proposed Medicare CAC Act has been used to great success across the globe to protect identity and secure transactions not only in health care, but in the financial services market as well. Known as "Chip & PIN", the smart card technology has revolutionized the way banks have reduced fraud and identity theft. As testimony to their security and efficacy in fighting fraud, American banks will be introducing Chip & PIN cards to the U.S. market beginning in 2013. Examples of success include:

- United Kingdom Chip & PIN smart card deployment for credit and debit card market. According to a UK Payments Administration reported in 2010, overall fraud losses in the UK fell by 67% and counterfeit card fraud losses have decreased by 77% since 2004, when Chip & PIN was adopted.

- France's Chip & PIN smart card deployment for credit and debit card market. The French banking association GIE CB reported in November 2010 that a fraud ratio of 0.072%, for a total 350 million (USD) – of which $140 million (USD) originated outside France. Five years ago 26% of the system wide fraud was attributed to the Internet and 74% attributed to the real world. Today the numbers are exactly the opposite with 75% attributed to Internet fraud and 25% to real world. GIE CB credits smart cards with reducing real world fraud. For a frame of reference, over 3.5 billion smart card transactions occur every year for a value of $597 billion (USD). There are 58 million smart banking cards in circulation in France (population 64m) with an average of 113 operations/transactions per user.

A trusted privacy and security tool for the Federal government

In addition to helping reduce fraud costs around the world, smart cards have been a reliable resource throughout the federal government for identity management and security for more than a decade. Designed on open standards approved by NIST, smart cards use non-proprietary technologies to help secure American's identity and security both home and abroad. Current federal smart card applications include:

- The Department of Defense Common Access Card. Today every federal agency, including the Department of Defense, utilizes secure smart cards to authenticate and verify users for building and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation.

- The U.S. Passport. Developed by the State Department and the Government Printing Office, all new passports include a secure smart card computer chip embedded in the back cover. Included to thwart passport counterfeiters, the secure chips protect American citizen's personal information in a manner that prevents tampering and eavesdropping. Since the first year of deployment, 2005, the State Department issued over 75 million ePassports containing the secure smart card chip.

- The Federal Emergency Management Agency's First Responders Authentication Credential (FRAC). In order to ensure local and state emergency response officials are able to collaborate to ensure the public's safety, many identity management challenges must be overcome. The FRAC card meets the task by allowing for interoperability between local, state, and federal first responders. So far, nine states have taken the lead to deploy FRAC credentials for first responders, with many more on the way. It should be noted that all doctors and nurses are considered first responders; as such a Medicare CAC provider card could serve double duty as a FRAC credential, even further reducing implementation costs.

- The American Medical Association/Centers for Disease Control Health Security Card. The American Medical Association's Center for Public Health Preparedness and Disaster Response is working with Center for Disease Control and FEMA to develop a pilot program to show the benefit of a Health Security Card based on smart card technology for patients in the event a disaster or health emergency. Preliminary findings from the pilot excises show 90% of patient using the smart cards rated the care they received as good to excellent, with 75% affirming care as very good or excellent. In December the AMA will issue a final report on the smart card pilot.

WHAT ARE THE COSTS OF IMPLEMENTING MEDICARE CAC?

Recently, the Smart Card Alliance, an industry non-profit 501 (c)(3) education foundation and trade association, worked with an independent auditor to determine the cost of deploying a smart card based Medicare card system for both providers and beneficiaries *(see attached, DeLeon & Stang Medicare Report)*. The audit was completed in March 2012 with the intent to assist Congress and the Centers for Medicare and Medicaid Services in their efforts to understand the true cost and actual savings of a nation-wide Medicare CAC deployment.

The audit found there are many different elements that must be considered as part of a national Medicare CAC deployment. Because the system will determine real-time eligibility of both providers and beneficiaries, it requires more than just the use of a smart card. Backend infrastructure and readers must be accounted for in any cost estimate. The estimate accounts for 2.6 million providers and 48 million beneficiaries for an overall total of 50.6 million participants.

Because providers will be going through an enrollment process and their biometric information will need to be captured the cost per provider within the system is estimated to be $31.08 per provider. For the beneficiary, the cost is somewhat less, $14.57 per beneficiary, because the beneficiary will receive their smart card via U.S. mail without the requirement of enrollment of biometric capture. The PIN code for the beneficiary could come pre-set as the last four digits of their Social Security number and could easily be changed, if the beneficiary desired upon first use. The total cost for nationwide deployment of Medicare CAC system averages out to $24.24 per participant for a grand total of $1.3 billion for full deployment. These costs are completely inclusive for full deployment and should be evaluated against the return in reductions in fraud, waste and abuse.

WHAT IS THE RETURN ON INVESTMENT AND WHAT IS IT BASED ON?

The Department of Justice estimates that fraud within the Medicare system costs American taxpayers over $60 billion per year. According to the General Accountability Office (GAO) in 2010 improper payments within Medicare were $48 billion per year. Senator Tom Coburn (R-OK) provided estimates during a March 2, 2011 Senate Finance Committee hearing entitled *Preventing Health Care Fraud: New Tools and Approaches to combat Old Challenges*, fraud and improper payments in the Medicare and Medicaid programs to cost taxpayers between $100 billion - $120 billion per year. Looking at the problem from any prospective, there is a lot of money at stake.

Based on savings reported by the UK, France, Germany and Taiwan across both the healthcare and financial services industries (noted above), it is clear that the use of smart card-based solutions led to a reduction in overall fraud losses upwards of 70%. While the Secure ID Coalition believes that the smart card-based Medicare CAC program will be able to deliver similar results, it is entirely reasonable to assume – at the very least – a cost savings of at least 50%, representing well over $30 billion in eliminated fraud annually at the current rate of fraud. This conservative estimate is further reinforced by the DOD's confirmation of a 46% reduction in cybersecurity attacks on the first day of deployment of the CAC card for computer access.

RECOMMENDATIONS

- Because the Medicare program is unique, deploying pilot programs or demonstration projects will be an important part of any successful smart card implementation. Five pilot projects in areas where there is a significant amount of fraud will help to identify the specific needs of the Medicare community. These areas could include specific states or regions, similar to metro regions, prioritized by risk categories.

- Planning is a critical part of any pilot program. It is the recommendation of the Secure ID Coalition that the Secretary of HHS be given enough time to plan for the success of the pilots, with a minimum of one year for mapping prior to implementation. Within the mapping period a process by which HHS/CMS establishes metrics to quantify reductions in fraud, waste and abuse must be clearly defined. Further, details of how beneficiary and provider privacy will be protected must be addressed.

- Assuring the interoperability of the new Medicare CAC hardware with existing practice management software systems will also be an important part of the pilot program. Claims are increasingly submitted through electronic interfaces; when including authenticated receipts of rendered services from the new Medicare CAC hardware, claims will be easier to verify by CMS, thus further reducing fraudulent payments and expediting audits. Since the private sector is tasked with the development and implementation of these practice management (PM) systems, the pilot program should be developed to report the essential data needed for determining how best to integrate Medicare CAC hardware into daily medical management practices.

- In order for pilots to provide the requisite amount of data, detailed information about usability, and specific measurable costs and benefits, a minimum duration of eighteen months is recommended for the pilot programs.

- Success of the pilot program will be determined by the established metrics defined prior to the start of the pilot program. Once completed HHS/CMS will be able to verify potential cost savings and benefits and determine the viability of a nationwide deployment without further direction from Congress.

- Once the pilots are completed, HHS/CMS will be able to assess the pilot data and design a nationwide Medicare smart card program that meets the needs of providers, beneficiaries and tax payers.

- Implementing a nationwide program of this scope should be done methodically and over time as to not overload HHS/CMS.

CONCLUSION

It's everyone's desire to see both the Medicare and Medicaid programs not only survive, but thrive. The cost of waste, fraud and abuse in these systems not only eat away at our tax reserves, but also forces federal and state authorities to spend tens of millions of dollars every year in law enforcement and prosecution costs. It only makes sense to stop the fraud before it happens. In this case, that means implementing a secure smart card to verify and authenticate valid Medicare and Medicaid users at the time of the transaction.

Smart cards are not only a globally recognized tool to help eliminate medical and financial fraud, but a trusted tool of the federal government in assuring identity across a number of critical applications. If Congress were to implement a smart card technology solution – such as described in the Medicare Common Access Card Act – it would have the potential to save American taxpayers over half of the estimated $60 billion per year cost of fraud. With over 48 million seniors, that comes out to approximately $1,250 of fraud per recipient per year. However, for a one-time investment of less than $25 per beneficiary, the federal government will realize a cost savings of over $612.50 per beneficiary per year – a return on investment 24 times over.

Everyone in Congress wants to preserve Medicare for the next generation of beneficiaries; Medicare CAC does this without having to raise taxes, eliminate benefits, or cut reimbursements. In our opinion, this is the best outcome of all possible solutions.

Mr. Chairman, Ranking Member, and Members of the Committee: the Secure ID Coalition stands ready to assist Congress in helping save the Medicare and Medicaid programs. We look forward to working with you and answering any questions you may have.

QUESTIONS & ANSWERS

If the beneficiary does not have their card, will they be denied access to care?
Absolutely not. CMS will need to establish a policy for how to process claims that are outside of the validated and authenticated Medicare CAC system.

Some cards will get lost, whether it's because of illness or just plain forgetfulness; it happens today in every program. This is not a technology issue, but a question of policy on how CMS would treat billings that have not been authenticated. In the case of beneficiaries who need to have a caretaker or legal guardian tend to their medical needs because they cannot communicate, a special caretaker credential could be issued to them.

How will personal privacy be protected using a smart card?
Both privacy and security must be considered fundamental design goals for any personal ID system and must be factored into the specification of the ID system's policies, processes, architectures, and technologies. The use of smart cards strengthens the ability of the system to protect individual privacy and secure personal information.
Unlike other identification technologies, smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes
- Segregate multiple applications on the card
- Support multiple single-purpose IDs
- Provide authentication of other system components
- Provide on-card matching of cardholder verification information
- Implement strong security for both the ID card and personal data

Smart cards trust nothing until proven otherwise. For example, smart cards can require cardholders to authenticate themselves first (with a PIN or biometric) before the cards will release any data. And smart cards support encryption, providing patient data privacy and enabling at-home or self-service applications in suspect or untrusted environments to be secure.

The smart card's embedded secure microcontroller provides it with built-in tamper resistance and the unique ability to securely store large amounts of data, carry out own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

In case a beneficiary card is lost, how secure is one's personal information?
If the card is lost, the data on the card is secure and not readable without the individual's PIN code. Further, all information stored in the card cannot be read unless accessed via an authorized, authenticated reader. An attempt to hack the chip on the card would destroy the information in the process, because the chips are designed to shut down under brute force

attacks. Once the card is reported lost or stolen the system will no longer recognize it and it becomes completely useless. One of the significant benefits that will reduce medical ID theft is that the card will no longer have the beneficiary's social security number printed on it.

In the case of beneficiaries seeking care outside their home region, how will the cards work?
This is an issue that exists today with paper Medicare cards containing SSNs in full view. The secure Medicare smart cards will work in any authenticated provider reader and benefits will be fully available nation-wide under existing Medicare services guidelines. During the pilot program, CMS would treat beneficiaries seeking care outside their home region under the same polices as if the beneficiary had lost their card.

Would a smart card program work with other program integrity efforts CMS has already deployed?
A smart card program will complement existing programs initially and, over time, the SIDC anticipates CMS would do away with some of the reactive initiatives underway due to the success of the smart card program to reduce fraud, waste and abuse in the system. Unlike the programs currently underway that search for fraud after the transaction has been process and the money disbursed, the smart card program is a proactive fraud prevention approach. To date, no proactive initiatives have been put forth by CMS.

APPENDIX

ADDITIONAL RESOURCES

- Smart Cards and Biometrics in Healthcare Identity Applications, Smart Card Alliance Healthcare Council white paper, May 2012
- Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications, Smart Card Alliance Healthcare Council brief, December 2011
- Effective Healthcare Identity Management: A Necessary First Step for Improving U.S. Healthcare Information Systems – A Smart Card Alliance Brief for Government Policy Makers and Other Stakeholders, Smart Card Alliance Healthcare Council and Identity Council brief, March 2009

ATTACHED DOCUMENTS

- Secure ID Coalition, *Medicare Common Access Card: How Does It Work*, 2012.
- DeLeon & Stang Certified Public Accountants and Advisors, *Smart Card Alliance Projected Schedule of Costs To Deploy Secure ID Card and Related Fraud Reduction Cost Savings and Return on Investment with Independent Accounts' Report,* June 27, 2012.
- *AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries*, September 14, 2011.
- Lawrence Carbonaro, *Converting to LifeMed*, Memorial Hospital of Conway, New Hampshire, 2012. (Memorial Hospital report on savings realized from conversion to LifeMed, a smart card-based health information system.)
- Theresa Min-Hyung Lee, *Comparative Study of Taiwanese Health Care System*, *in* The Ampersand Journal, Issue IV 42 (McGill University), 2011.

How it works

Medicare Common Access Card

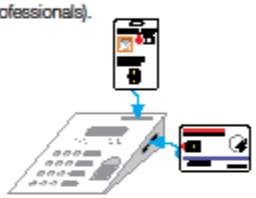
1 **Medicare beneficiaries and service providers receive a secure ID card.**

The smart card contains a computer chip that fights fraud and protects privacy.

What's stored on the ID card:

- A unique Medicare identity.
- A digital picture of the healthcare professional.
- A PIN code (beneficiaries) or biometric (professionals).
- Match-on-card software: PIN or biometric stays in the card.

2 **At the doctor's office, both the ID cards are inserted into the reader. The chip on the card electronically confirms the card is legitimate.**



3 **The doctor confirms his or her identity by touching the biometric reader, and the beneficiary by entering a PIN code, proving both were there.**

4 **Transaction is confirmed and a secure authenticated information packet is sent to the payment processor.**

What is match-on-card biometric technology?

1. During registration, the system generates a mathematical value based on the fingerprint. This value, called a template, is used for identity matching, not the actual fingerprint image.
2. The biometric template is encrypted and securely stored in the smart card chip.
3. During a transaction, the terminal scans the finger, generates a template and sends it to the card.
4. The match-on-card software compares the two template numerical values to see if they match. If they match, the person making the transaction is the cardholder.

Advantages

- The encrypted fingerprint biometric value never leaves the card.
- Privacy is assured because the full fingerprint image is never stored.
- Cardholder carries their biometric and PIN information with them.
- Simplifies networking, improves security and reliability, and enhances privacy. Eliminates the need for an online centralized database.

Common Access Card fights fraud, protects privacy

- Stops phantom billing. The beneficiary, the provider and their Medicare ID cards must be present to process a transaction.

- Prevents card passing. PIN code confirms patient identity.

- Protects privacy. Digital picture, PIN or biometric stays in the card.

- Because the Medicare card is a smart card, if the card is lost it can be deactivated remotely, protecting healthcare identity and information.

- Accurate identification and confirmation of eligibility of both beneficiary and service provider.

- Smart card security features prevent counterfeiting or altering ID cards and protect people's privacy and benefits.

- Privacy sensitive. Cardholders carry their PIN or biometric with them in the smart chip.

- With biometric, actual fingerprint images are not on the card, protecting privacy. Instead a mathematical value based on the person's finger is used to confirm identity.

Medicare Common Access Cards stop rampant Medicare fraud.

For more information contact the Secure ID Coalition | www.secureidcoalition.org | p:202-464-4000

SMART CARD ALLIANCE
PROJECTED SCHEDULE OF COSTS
TO DEPLOY SECURE ID CARD
AND RELATED FRAUD REDUCTION COST
SAVINGS AND RETURN ON INVESTMENT
WITH
INDEPENDENT ACCOUNTANTS' REPORT

DeLeon & Stang
Certified Public Accountants and Advisors

100 Lakeforest Boulevard
Suite 650
Gaithersburg, MD 20877
P: 301-948-9825
F: 301-948-3220
www.deleonandstang.com

Allen P. DeLeon, CPA, P.C.
Richard C. Stang, CPA, P.C.
Jeanie Price

INDEPENDENT ACCOUNTANTS' REPORT

Smart Card Alliance
Washington, DC

We have examined the accompanying projected Schedule of Costs to Deploy a Secure ID Card Within the U.S. Medicare System, and the Schedule of Projected and Fraud Reduction Cost Savings of Deployment of a Secure ID Card Within the U.S. Medicare System and the Related return on Investments (ROI) as of February 13, 2012, which has been prepared by Smart Card Alliance. Smart Card Alliance's management is responsible for the projections, which were prepared for the purpose of providing educational information relevant to proposed legislation being drafted by the U.S. Congress. Our responsibility is to express an opinion on the projections based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the projection. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, the accompanying projections are presented in conformity with guidelines for presentation of a projection established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projections assuming:

1. The deployment costs are accurately projected by using an average of the projected deployment costs based on a survey of six companies which specialize in deployment of similar secure ID cards for similar purposes in the U.S. and foreign countries, and other estimates of deployment costs made by the Smart Card Alliance, Health Council Members.
2. The quantity of projected users of the secure ID card are accurately estimated using U.S. Department of Health and Human Services (HHS) information as described in the projection.
3. The cost savings are accurately projected by using cost savings of similar programs in the U.S. and foreign countries, as described in the projection.
4. The return on investment (ROI) is accurately projected by using the projected cost savings and applying it to the estimated current levels of Medicare fraud.

However, even if the assumptions referred to above are accurate, there will usually be differences between the projected and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

The accompanying projection and this report are intended solely for the information and use of (1) members of management of the Smart Card Alliance and (2) the U.S. Congress and related US government agencies, in connection with proposed legislation related to the deployment of secure ID cards, and are not intended to be and should not be used by anyone other than these specified parties.

DeLeon & Stang
DeLeon & Stang, CPAs and Advisors
Gaithersburg, Maryland
June 27, 2012

SMART CARD ALLIANCE
Schedule of Costs to Deploy a Secure ID Card
Within the U. S. Medicare System
February 13, 2012

National Rollout

Professionals working at hospitals, physician's offices, Medical equipment suppliers, nursing homes, assisted living residences, mental health professionals and pharmacies who require ID cards.	Quantity	Source of information
TOTAL PROFESSIONALS	**2,624,884**	National Plan and provider Enumeration System Statistics 5/05 - 7/11

Cards Required	Quantity	Price Per Unit	Total	
Professionals	2,624,884	$4.17	$10,932,642	See quantity above
Beneficiaries	48,000,000	$1.00	$48,091,200	Industry estimate
TOTAL CARDS	**50,624,884**	**$1.17**	**$59,023,842**	

Medicare Cost Summary

Providers and Suppliers	Users	Average Cost Per Person	Total	Comments
Enrollment of Providers and Suppliers	2,624,884	$12.82	$33,637,888	Cost to enroll everyone, prove licensing
Background Investigation (Vetting)	2,624,884	$0.00	$0	Already included in existing processing costs
Biometric AFIS Database	2,624,884	$0.59	$1,557,869	Checking against data base
Large Systems Integrator (LSI)	2,624,884	$0.76	$1,994,912	Allow cards to be read in existing CMS system
Digital Certificate - Level 3 MHW Assurance	2,624,884	$1.01	$2,638,008	Electronic version of ID recognition
Card Stock	2,624,884	$4.17	$10,932,642	Physical card from above
Card Issuance & Fulfillment	2,624,884	$3.25	$8,522,123	Mailing out cards
Card Manufacturer Professional Services	2,624,884	$0.10	$262,488	Consulting
Middleware/ Strong Authentication Server with Connect	2,624,884	$6.62	$17,363,608	Connect to software
Software Licensing	2,624,884	$1.25	$3,283,730	Licensing of vendor software
Card Management System (CMS)	2,624,884	$0.33	$853,087	Integration
Identity Management System (IDMS)	2,624,884	$0.21	$538,101	Integration
PROVIDER & SUPPLIER TOTAL	**2,624,884**	**$31.08**	**$81,584,457**	

Page 2

SMART CARD ALLIANCE
Schedule of Costs to Deploy a Secure ID Card
Within the U. S. Medicare System
February 13, 2012 (Continued)

Beneficiaries	**Users**	**Per Person**	**Total**	
Digital Certificate plus Class 2 Identity Proofing	48,000,000	$2.82	$135,200,000	PIN required to activate
Card stock	48,000,000	$1.00	$48,091,200	Electronic version of ID recognition
Card Issuance & Fulfillment	48,000,000	$3.44	$165,280,000	Physical card from above
Card Manufacturer Professional Services	48,000,000	$0.07	$3,120,000	Mailing out cards
Middleware/ Strong Authentication Server with Connect	48,000,000	$0.23	$11,040,000	Consulting
Large Systems Integrator (LSI)	48,000,000	$5.24	$251,520,000	Connect to software
Software Licensing	48,000,000	$1.26	$60,331,200	Licensing of vendor software
Card Management System (CMS)	48,000,000	$0.32	$15,120,000	Integration
Identity Management System (IDMS)	48,000,000	$0.21	$9,840,000	Integration
BENEFICIARY TOTAL	**48,000,000**	**$14.57**	**$699,542,400**	

Readers and Terminals	**Quantity**	**Per Unit/Per Person**	**Total**
USB Contact Readers	170,537	$7.50	$1,279,025
Dual Slotted Terminals (German model)	103,000	$162.50	$16,737,500
Biometric (Fingerprint) Readers	170,537	$80.00	$13,642,933
	444,073	**$71.29**	**$31,659,458**

Activation Kiosks	**17,500**	$23,666.61	$414,165,675	To change PIN, add photo, activate card
GRAND TOTAL (National Rollout)	**50,624,884**	**$24.24**	**$1,226,951,990**	
Annual Maintenance of Total Cost	25%		**$306,737,997.60**	% of total costs estimate

SMART CARD ALLIANCE
Schedule of Projected Fraud Reduction Cost Savings of
Deployment of a Secure ID Card in the U. S. Medicare System
And the Related Return on Investments

Fraud		**Year 1**	**5 Yr. aggregate**	**10 yr. aggregate**
Current Situation		$60,000,000,000	$300,000,000,000	$600,000,000,000
Fraud Reduction Percentage		**Savings**		
	10%	$6,000,000,000	$30,000,000,000	$60,000,000,000
	20%	$12,000,000,000	$60,000,000,000	$120,000,000,000
	33%	$19,800,000,000	$99,000,000,000	$198,000,000,000
	40%	$24,000,000,000	$120,000,000,000	$240,000,000,000
	50%	$30,000,000,000	$150,000,000,000	$300,000,000,000
	66%	$39,600,000,000	$198,000,000,000	$396,000,000,000
	70%	$42,000,000,000	$210,000,000,000	$420,000,000,000
	80%	$48,000,000,000	$240,000,000,000	$480,000,000,000
	90%	$54,000,000,000	$270,000,000,000	$540,000,000,000
Return on Investment				
Fraud Reduced by				
	10%	$4,466,310,012	$27,239,358,022	$55,705,668,034
	20%	$10,466,310,012	$57,239,358,022	$115,705,668,034
	33%	$18,266,310,012	$96,239,358,022	$193,705,668,034
	40%	$22,466,310,012	$117,239,358,022	$235,705,668,034
	50%	$28,466,310,012	$147,239,358,022	$295,705,668,034
	66%	$38,066,310,012	$195,239,358,022	$391,705,668,034
	70%	$40,466,310,012	$207,239,358,022	$415,705,668,034
	80%	$46,466,310,012	$237,239,358,022	$475,705,668,034
	90%	$52,466,310,012	$267,239,358,022	$535,705,668,034

Page 4

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction Savings of Secure ID Card
February 13, 2012

NOTE 1 - NATURE AND PURPOSE OF ORGANIZATION

The Smart Card Alliance is a non-profit organization, located in Washington DC and tax exempt under section 501 (c) (6) of the Internal Revenue Code (IRC). Its mission is to accelerate the widespread adoption, usage and application of smart card technology in North America, by bringing together users and technology providers in an open forum to address opportunities and challenges for the industry. Its membership consists of companies and individuals in technology companies, federal, state and local governments, academic institutions, consulting companies and Latin American companies and institutions. The Organization conducts conferences, prepares publications, and provides resources to its members in furtherance of its purpose.

NOTE 2 - SPECIFIC PURPOSE OF THE PROJECTIONS

The purpose of this report is to provide projections related to (1) the estimated costs of the deployment of a secure ID card in the U.S. Medicare system to the U.S. Congress, (2) the estimated fraud reduction cost savings and return on investment (ROI), in relation to proposed legislation to conduct a pilot program.

NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS

Certain assumptions were used in developing the projections. The projections are only as reliable as the accuracy of the assumptions. Even if the assumptions described in this report are accurate, there will usually be differences between projected results and actual results, because events and circumstances frequently do not occur as expected and those differences could be material. The underlying assumptions used to develop the projections in the report are:

1. The costs of deployment of a secure ID card are based on the average cost projections developed from a survey of technology companies which are members of the Smart Card Alliance. The survey consisted of six companies, and the projected costs are an average of the costs projected by these companies. Some companies did not provide cost information in all cost areas. Some of the estimates of deployment costs were made by the Smart Card Alliance and Healthcare Council Members, and not directly from the survey results. The surveyed companies; cost projections are only as accurate as the projections provided by the survey. Since the overall deployment costs are based on the cost per user multiplied by the number of projected users, the actual deployment costs could differ significantly from the projected costs if the actual cost per user is different from the projected cost per user.

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction
Savings of Secure ID Card (Continued)
February 13, 2012

NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS (Continued)

2. The quantity of projected users of the secure ID card was determined from information obtained from the National Plan and Provider Enumeration System (NPPES), a division of the Centers for Medicare and Medicaid Services (CMS) of the U. S. Department of Health and Human Services (HHS). Since the projected costs of deployment of a secure ID card is based on the cost per user multiplied by the number of projected users, the accuracy of the number of users is a material component in the total cost projection. The NPPES information is generally considered to the most current and accurate estimate of the number of users of a secure ID card. However, the overall deployment costs relies heavily on the quantity of users, and may differ significantly from the actual costs if the actual number of users differs from the projected number of users.
3. The fraud reduction cost savings is presented at various assumed percentages of savings. It is assumed that the current Medicare fraud is approximately $60 billion per year. The fraud reduction cost savings is based on cost savings of similar programs using other applications of the secure ID card and deployment of a secure ID card in other countries whose medical systems and related regulations differs from those in the U.S. While management believes that the fraud reduction cost savings reported by other secure card applications and deployments in other countries is a reasonable estimate of the fraud reduction cost savings that would be achieved in the U.S., material differences could exist which would affect the total cost savings.
4. The projected return on investment (ROI) is also presented at various assumed fraud reduction percentages. The projected ROI is computed by subtracting the total projected fraud cost savings, at each assumed savings percentages, from the projected deployment costs. Since the total projected deployment costs and the projected fraud reduction savings are based on the assumptions described above, the ROI is based on, and subject to, these assumptions. If the total projected deployment costs and/or the total projected cost savings differ materially from the actual results, the actual ROI will differ materially from the projected ROI.

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction
Savings of Secure ID Card (Continued)
February 13, 2012

NOTE 4 - LIMITATIONS OF USE OF THE PROJECTIONS AND SPECIFIED PARTIES

The projected information contained in this report is intended for a specific purpose and use, it is not intended that the projections be used for any other purposes or uses. Further, this report is intended for use by (1) Members of the Smart Card Alliance, (2) the U.S. Congress and related U. S. government agencies related to proposed legislation concerning a pilot program for deployment of a secure ID card in the U.S. Medicare system, the use of this report is not intended to be used, and should not be used, by any other parties other than the specified users.

AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

AARP today endorsed the Medicare Common Access Card Act of 2011

From: Press Center | September 14, 2011

FOR IMMEDIATE RELEASE
September 14, 2011

CONTACT:
AARP Media Relations, 202-434-2560

AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

WASHINGTON – AARP today endorsed the Medicare Common Access Card Act of 2011 in a letter to U.S. Senators Mark Kirk and Ron Wyden as well as U.S. Representatives Jim Gerlach and Earl Blumenauer. The bill will create a secure Medicare identification card pilot program for beneficiaries located in five geographic areas nationwide. This bipartisan and bicameral piece of legislation introduced today will replace paper Medicare cards with secure cards that carry the personal information electronically of individuals in the program.

Excerpts of the letter of support from Joyce A. Rogers, AARP Senior Vice President, are below:

"On behalf of AARP's millions of members, we are pleased to endorse the Medicare Common Access Card Act of 2011. Your legislation will create a secure card pilot program under the Medicare program.

"Older Americans are particularly vulnerable to the dangers of identity theft. Your legislation will pilot a program to replace the current paper Medicare card with a smart card that would store the beneficiary's personal information electronically on a computer chip, and would require both beneficiaries and providers to confirm receipt of services at the time services were provided. Similar technology currently exists for Department of Defense personnel.

"Your legislation not only provides enhanced information security, but will also help to reduce fraud in the Medicare program by verifying the identity of both Medicare beneficiaries and providers. Medicare dollars should be spent on necessary services and not lost to fraudulent activities."

For a copy of the full-text of the letter, please contact AARP Media Relations by phone at (202) 434-2560 or via email at media@aarp.org.

About AARP:
AARP is a nonprofit, nonpartisan organization with a membership that helps people 50+ have independence, choice and control in ways that are beneficial and affordable to them and society as a whole. AARP does not endorse candidates for public office or make contributions to either political campaigns or candidates. We produce AARP The Magazine, the definitive voice for 50+ Americans and the world's largest-circulation magazine with nearly 35 million readers; AARP Bulletin, the go-to news source for AARP's millions of members and Americans 50+; AARP VIVA, the only bilingual U.S. publication dedicated exclusively to the 50+ Hispanic community; and our website, AARP.org. AARP Foundation is an affiliated charity that provides security, protection, and empowerment to older persons in need with support from thousands of volunteers, donors, and sponsors. We have staffed offices in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

http://www.aarp.org/about-aarp/press-center/info-09-2011/aarp-joins-bipartisan-effort-to-prevent-identity-theft-of-medicare-beneficiaries.print.html

Converting to LifeMed

By: Lawrence Carbonaro
Director, Purchasing, Patient Access & HIS

The Memorial Hospital, North Conway, NH **(35 beds, 100,000 annual patient visits and over $300,000 in administrative savings annually, not including the marketing advantages)**

- **Decreased admissions error rate from 6% to less than 1%** *We average 1500 registrations a week, thus 90 records that used to require manual intervention to fix before billing; with LifeMed we no longer require that effort.)*
- **Elimination of clip board and paper** *(We went paperless as a result of LifeMed. We used to print a cover sheet to give to the patient with each registration, this is no longer required. 156 cases of paper plus toner are no longer used, no shredding or storage.)*
- **Reduced duplicate records from 7% to less than 1%** *(an annual cost savings of **$35K-$55k** for scrubbing records. No numbers reported for medical errors due to incorrect chart)*
- **Reduced admission time from 22 minutes to less than 3 minutes** *(average salary equaling $18.13 an hour and a average saving of 19 minutes equals a soft cost saving of $5.74 per patient times 100,000 patents annually. Registration saving of **$574,000** of annual employee payroll minutes allowing Memorial to redirect staff to other productive tasks, like accurate insurance billings, etc. - LifeMed soft projection).* See reduced staff below
- **Reduced medical record error from 7% to less than 1%** *(unreported cost savings but includes billing losses, medical procedure losses, medical errors, lawsuits, etc)*
- **Reduced PAC System errors to less than 1%** *(Hard to quantify but PACs errors were occurring about 150 annually, now they are rare. Pacs administrator time was 3+ hours to fix each error. About **$25K** savings, assumed pay would be greater than $100K)*
- **Reduced full time staff requirements from 21 to 15** *(Annual savings equates to **$224,640** using a burdened salary of $37,440 annually).*
- **Decreased insurance A/R from 55+ to 42 days** *(unreported saving; Current days are still reducing in A/R and is now below 41 days).*
- **Increased Press-Ganey patient satisfaction by 10% within first 60 days** *(Memorial's now in the top **5%** of all hospitals with satisfaction in registration - this was a major issue as our patient dissatisfaction began at admission even before the patient saw an employee or clinician. Patient satisfaction influenced patient and employee retention and employee gratification).*

Areas of Savings not reported or financially measured as of the date of these Administrative Measures:

- Patient Satisfaction Increase
- Diminished Registration Errors
- Diminished in Duplicate Records
- Diminished in Record Errors
- Elimination of Registration Paper
- Decreased Insurance A/R

Comparative Study of Taiwanese Health Care System
Theresa Min-Hyung Lee

The health care system of Taiwan is an exemplary model of how modern health care reform and major policy changes can bring about high quality universal health coverage to a country in a relatively short period of time. After years of consulting international experts in the health policy field and studying numerous health care systems around the world, Taiwan instituted its universal National Health Insurance (NHI) program in 1995, extending a comprehensive benefits package ranging from doctor visits, prescription drugs to even traditional Chinese medicine to 99 percent of the Taiwanese population. The Taiwanese receive their health care services in a very timely manner with minimal wait times, and the result is that the overall population remains both healthy and happy with the health care system of their country.

Most of us are also satisfied with the health care we receive here in Canada (Statistics Canada, 2008), perhaps in lieu of the health care reform debate raging in the United States. Yet, we have had the unpleasant experience of sitting in the waiting room of the doctor's office for countless number of hours, or perhaps know of someone who has had to wait months to receive treatment or diagnosis that should not have been delayed. The Canadian government is quite aware of this problem challenging both the health care providers and receivers alike, and is making an effort to find a solution. One such initiative is the investment of 4.5 billion dollars into the Wait Time Reduction Fund since 2004 (Health Canada, 2004).

With all of this in mind, I leapt at the opportunity to partake in a Public Health Exchange program through McGill's Global Health Programs to observe best practices adopted by Taiwan's health care systems, and how it came to serve its citizens so effectively and efficiently.

The expansion of health care in Taiwan mirrors its rapid economic development. After a strong economic growth of more than twenty years, the public of Taiwan demanded a better health insurance coverage in the 1980s, leading to a full-fledged national health insurance program. The new health insurance coverage arose from years of in-depth studies of health care systems from other nations. The health reform resulted in the NHI, which is now a government-run, single-payer system with universal coverage similar to that of Canada's. Prior to the establishment of NHI in 1995, 41 per cent of the Taiwanese population was uninsured – the majority of the uninsured were young children and seniors, whose need for health care is usually the highest. As a result of the mandatory enrollment, the reform has since brought insurance to 99 per cent of citizens and legal residents, and increased the health care utilization rates of the uninsured up to par with those of previously insured populations (Cheng 2003).

Despite several similarities with the Canadian health care system as a whole, there are some notable differences between the two systems. Firstly, Taiwan's health care coverage is more comprehensive. It covers services that Canadians are usually pay out-of-pocket, or through supplemental health insurance. These services include prescription drugs, dental care, vision care and traditional Chinese medicine (Cheng 2003).

Secondly, patients are free to see doctors of any specialty without going through a referral or 'gatekeeper' system. There are also no limitations on the type of hospital that from which the patients can receive their health care. Due to the absence of a gatekeeper system, there is no need to first see your primary healthcare provider to receive a referral to see a specialist. As a result, there is virtually no waiting list for a visit to the doctor's office. There is also freedom to choose between health care facilities, ranging from small public health clinics to large private hospitals that offer comfort with luxurious décor.

Upon observing and learning about many health care facilities (including public and private clinics, large teaching hospitals, major public hospitals and private hospitals alike, to a psychiatric hospital, a Traditional Chinese Medical hospital and a regional Centre for Disease Control), and discussing with and listening to doctors, nurses, professors and medical students, the facilities appeared to be spectacular, well-equipped with modern technology; and the breadth of services available to the Taiwanese population presented was truly impressive.

With high health indicators comparable to any developed nation – infant mortality rate of 5.26 per 1000 births; and life expectancy at birth of 75.34 years for men and 81.2 years for women (Central Intelligence Agency, 2010) – it was clear that Taiwan was providing health care that successfully sustains a healthy general population. Furthermore, a closer look at Taiwan's national health expenditure rates indicate that this was being achieved at a fraction of the cost of other nations: only 6 percent of Taiwan's GDP is spent on healthcare, compared to 10 percent for Canada and 16 percent for the United States (Organization for Economic Cooperation and Development, 2010). Since its implementation, NHI has had a public satisfaction rating ranging from 70 to 80 per cent, dipping low only in the years where new policies introduced higher insurance rates (Cheng 2003). It remained unclear how Taiwan managed to sustain a health care system achieving similar, if not better, results than that of Canada's and the United States'

The NHI is publicly funded and financed on income-based premiums as opposed to general tax revenues. The premiums are based on payroll taxes paid by the employer, the employee and the government in varying amounts depending on different population groups. Most people who are employed pay 30 per cent of the premium, while their employee pays 60 per cent and the government subsidizes the remaining 10 per cent. The self-employed pay 100 per cent of the premium, and individuals from a low-income household are fully subsidized by the government. For the employed, the total insurance premium is typically 4.6 per cent of their

wages (Underwood, 2009), as well, the taxes from tobacco excise tax and the national lottery revenues are injected/infused into the system (Bureau of National Health Insurance, 2010).

The cost of the services from providers is covered mainly through reimbursements from the NHI, but it is also partially covered by co-payments from users (Cheng, 2003). The NHI is also supplemented by a co-insurance system where the user pays a nominal co-payment to the health care provider upon the use of its services. Its purpose is to discourage overuse. This may be compared to how wait times stemming from the referral-system in Canada discourages unnecessary hospital visits. The co-payment is usually a few dollars, or a fraction of the true cost of the service provided. The amount is capped by the NHI to eliminate any concerns of bankruptcy resulting from an accumulation of the fees. It is also waived for catastrophic diseases, individuals from low-income households or remote areas, infants and veterans.

One problematic area of health care that the NHI has tackled progressively is implementing the universal coverage and assuring similar health status between the indigenous and marginalized populations, and the rest of Taiwan. In order to eliminate disparities regarding access to health care, NHI has approached both the demand and supply side. On the demand side, it ensured that the population at risk were provided with insurance, and exempted them from co-payment. On the supply side, it has implemented an Integrated Delivery System (IDS), and guaranteed income for physicians practicing in remote areas (Bureau of National Health Insurance, 2010). Although certain disparities still exist, policy tools such as IDS and rural payment bonuses contribute to continuous improvements (Chou, Huang et al., 2004).

Another innovation is the integration of traditional methods in a modern system. As traditional Chinese medical practice is an accepted form of medicine, and is a mainstream medical care in Taiwan. Chinese medicine is insured under the NHI. Traditional Chinese Medical (TCM) services ranges from acupuncture and fire cupping massages to medicinal herbs. It is believed to be effective in alleviation of many illnesses and disease, managing pain and promoting well-being. Traditional Chinese medicine is often used in conjunction with Western biomedicine (Chen, Chen et al. 2007) and accounts for six per cent of health expenditure on outpatient services in Taiwan (Bureau of National Health Insurance, 2010). However, not all TCM clinics are registered under the NHI, and standardization regarding the quality was not so straightforward.

As it turns out, the NHI began facing deficits in the late 1990s, relying on bank loans to pay health care providers. Between 1996 and 2009, NHI expenditures grew at an average of 5.27 per cent a year, exceeding NHI revenues with an average growth rate of 4.02 per cent a year (Bureau of National Health Insurance, 2010). The exceeding expenditures were a fault of the open-ended health insurance system relying on a Fee-For-Service (FFS) payment of the providers. The health care

providers performed unnecessary procedures and prescribed unnecessarily expensive, drugs at the expense of the NHI. Submission of false reimbursement claims was another example of misuse of the system (Cheng 2003).

Due to the competitive nature of FFS, physicians were called upon to see an overwhelmingly large volume of patients per day, leading to rushed visits and insufficient time to get a complete patient history or conducting a thorough exam, which could lead to misdiagnosis, improper treatment or delays in proper treatment. This led to a vicious cycle of doctors ordering frequent follow-ups, which contributed to higher patient volumes and shorter visits. Moreover, many patients were led to believe/feel that their problems were not adequately addressed, resulting in repeat visits and 'doctor shopping' – visiting numerous practitioners simultaneously, and seeking unnecessary care, or care that does not require specialists, all further impinging on the system (Gunde, 2004).

To address some of these issues, the NHI made a number of changes in how the health care providers were reimbursed. From 1998 to 2002, a global budget policy was imposed on different sectors, replacing the Fee-for-Service system. The Global policy set an expenditure cap for each sector, whereby services provided beyond the cap would be reimbursed at lower rates. The new policy incentivized health care providers to stay within their set budget. Global budgeting proved to be effective, and overall growth rates of per capita medical spending declined in nearly all of the health sectors in the early 2000s. However, it was an incomplete solution as the NHI continued to face ever increasing expenditures.

In 2004, the NHI implemented a Resource-Based Relative-Value Scale (RBRVS) into the physician fee schedule, where physicians were paid according to the "relative value" of services provided and the resources they consumed. It is based on the amount of physican-involving work that goes into the service, the practice expense associated with the service, and the professional liability expense for the provision of that service; also being adjusted according to the geographic region (American Association for Pediatrics, 2005).

The NHI continues to experiment with different methods of payment of provider. The most recent change to the heatlh care system was in 2010, where the NHI introduced a diagnosis-related-group reimbursement (DRG) scheme to pay physicians. Under this scheme, the physicans are reimbursed at a certain rate for different types of patients according to their primary diagnosis (Bureau of National Health Insraunce, 2009).

Further efforts to improve the quality of the NHI system led to the introduction of the IC (Integrated Circuit) Smart Card: a mandatory health card of sorts, but integrating innovative information technology. The Smart Card contains electronic data about the cardholder's personal identity, medical record, prescription history, remarks for catastrophic diseases, number of visits, administrative and expenditure information among other things (Smart Card Alliance, 2005). The introduction of

the Smart Card in 2002, had allowed Taiwanese hospitals and clinics to send electronic records on a daily basis to the Bureau of NHI, where the data is analyzed and audited on a regular basis. The Smart Card makes it possible to monitor high-utilization cases through patient profile analysis; prevent fraud from aberrant medical claims; and keeps surveillance of public hazards, tracking down suspects of communicable disease (Bureau of National Health Insurance, 2009).

The tracking of symptoms of communicable diseases is becoming increasingly important with the rise of pandemic disease, where persons infected must be identified and isolated as soon as possible to prevent the spreading of the infection. Although it is a relatively new system, preliminary results have indicated that the Smart Card has enormous potential to be a key tool in reducing infectious outbreaks, such as severe acute respiratory syndrome (SARS), through implementation of an on-line real-time mechanism for disease control, tracking and surveillance (Huang and Hou 2007).

Another major benefit from the use of Smart Card technology is the reduction in administrative costs due to improved administrative, billing and provider efficiencies. The technology has allowed for automatic operation of electronic transfer of medical records and bills, resulting in expedited reimbursements of providers. As the Smart Cards last for several years, it has also eliminated costs involved with frequent replacement of older health cards, which were previously made of non-durable material. As a result, Taiwan's health care system has the lowest administrative costs in the world, accounting for only two per cent of its total health expenditure. Comparatively, Canada spends 16 per cent of total health expenditures on administration and the United States spends 31 per cent (Woolhandler, 2003). The low administrative cost significantly contributes to how Taiwan has maintained the low rate of health expenditure spending over the accumulated GDP spending.

In spite of these efforts of new innovations and policy implementation, health care costs are still rising in Taiwan. The NHI's deficit is expected to reach $3.2 billion US dollars by the end of 2010 if effective measures are not put into place. The government could increase spending from its GDP by raising the premiums although it would cause public unrest in the process. But even so, the extra income generated from increased premiums will only be a temporary measure in keeping the balance and offsetting the existing deficit of $1.84 billion dollars US (Taiwan Today, 2010).

Taiwan is now looking overseas for other potential solutions. Medical tourism is a new and growing area in the world economy (Morgan, 2009) and it has come to the attention of the Taiwanese health care industry. In hopes of easing its growing deficit and financial burden, the Taiwanese government's Department of Health began planning distribution channels and marketing campaigns on medical tourism. Now, Taiwan brands itself as a home for first-rate medical care services (International Medical Tourism Journal, 2009). Taiwan has long been popular with its expatriate population as a medical-travel destination (Tung, 2010). However, the

market is expected to expand by several folds as Taiwan further opens its door to mainland China. With the recent lift of travel restrictions, 2009 alone brought 40,000 visitors from China to Taiwan to undergo health checkups and cosmetic surgery (Kastner, 2010).

Creating a system that is both financially sustainable and meets the needs of an evolving population is a fine balancing act with many factors. Taiwan will face health care challenges common to many other countries in the near future: an aging population; rising cost of the workforce in the medical health industry; and increasing costs of new technology and drug research and development.

The two weeks I spent in Taiwan taught me that there are no easy tricks to finding a solution to a problem. The development of the health care system is a continually evolving process that is sensitive to time, place, political and economic state of the country, and the needs of the people.

As it stands, the Taiwanese government is currently working on a 'second generation' NHI reformation, implementing new policies and strategies to make the health care system more sustainable (Bureau of National Health Insurance, 2010). Collaborating with other nations by sharing information on policy implications, research data, consultations and other innovations have led to the development and establishment of what is the NHI today. Further innovation and collaboration among nations can ensure that future steps taken to develop and to implement health care policies are more effective.

For now, Taiwan and the NHI stands as a successful case of how a nation was able to successfully established a universal health care coverage for the entire nation – almost from ground up. The system offers, at an affordable cost to the users, easy access to comprehensive health care of high quality. Despite some of the financial weaknesses it has shown and the downfalls it has faced in the last fifteen years, it is an example of how a government can strategically manage its resources in order to serve its people effectively; providing access to health care to those who need it most.

References

American Academy of Pediatrics (2008) "Application of the Resource-Based Relative Value Scale System to Pediatrics".
http://aappolicy.aappublications.org/cgi/reprint/pediatrics;122/6/1395.pdf

Bureau of National Health Insurance (2010). "National Health Insurance in Taiwan".
http://www.nhi.gov.tw/webdata/AttachFiles/2010NHIprofile_990503.pdf

Central Intelligence Agency. (2010, Nov). Taiwan. Retrieved November 2010, from The World Factbook: https://www.cia.gov/library/publications/the-world-factbook/geos/tw.html

Chen, F.-P., T.-J. Chen, et al. (2007). "Use frequency of traditional Chinese medicine in Taiwan." BMC Health Services Research 7(1): 26.

Cheng, Tsung-Mei (2003). Taiwan's new national health insurance program: genesis and experience so far. Health Affairs , 22 (3), 61-76.

Chou YJ, Huang N, Chang HJ, Yip W; AcademyHealth. Meeting (2004 : San Diego, Calif.). "National Health Insurance and Disparities in Access to Care in Rural Areas: A population-based study in Taiwan." Abstr Academy Health Meet. 2004; 21: abstract no. 1049. Retrieved November 2010 from http://gateway.nlm.nih.gov/MeetingAbstracts/ma?f=103624083.html

Gunde, Richard. (Sept 30, 2004). "Healthcare in Taiwan: Opportunities and Success." UCLA International Institute. Retrieved 2010 from http://www.international.ucla.edu/article.asp?parentid=15333

Health Canada. (2004, September 16). "First Ministers' Meeting on the Future of Health Care 2004: A 10-year plan to strengthen health care." Retrieved November 2010, from http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2004-fmm- rpm/index_e.html

Health Canada (2008). "Healthy Canadians: Federal Report on Comparable Health Indicators 2008" http://www.hc-sc.gc.ca/hcs-sss/pubs/system-regime/2008-fed-comp-indicat/index-eng.php

Huang, J.-W. and T.-W. Hou (2007). "Design and prototype of a mechanism for active on-line emerging/notifiable infectious diseases control, tracking and surveillance, based on a national healthcare card system." Computer methods and programs in biomedicine 86(2): 161-170.

IHS Global Insight (March 8, 2010). "NHI to See over US $3—bil. Deficit in Taiwan, Health Minister Announces Resignation." Retrieved November 2010 from http://www.ihsglobalinsight.com/SDA/SDADetail18372.htm

International Medical Travel Journal (Dec 11, 2009). "TAIWAN: Taiwan government to promote inbound medical tourism". http://www.imtj.com/news/?EntryId82=172651

Kastner, Jens (October 5, 2010). "Taiwan's Medical Tourism Boom". Asia Sentinelhttp://www.asiasentinel.com/index.php?option=com_content&task=view&id=2736&Itemid=192

Lu, R. J.-F., & Hsiao, W. C. (2003). "Does universal health insurance make health care unaffordable? Lessons from Taiwan." Health Affairs , 22 (3), 77-86.

Morgan, David. (October 2009) "Tracking the growth in Medical Tourism: OECD helps Ministers shape the debate." Organization for Economic Cooperation and Development. Health division.

Nelson, Chris (March 2007). "Taking the Cure: Medical Tourism." Taiwan Panorama P. 34 Retrieved November 2010 from http://www.sino.gov.tw/en/show_issue.php?id=200739603034e.txt&cur_page=1&listype=text&table=2&h1=Finance%20and%20Economy&h2=&search=&height=&type=&scope=&order=&keyword=&listPage=&num=&year=2007&month=03

Organization for Economic Co-operation and Development. (2010) OECD Health Data 2010

Reid, T.R. (2008). Taiwan Takes Fast Track to Universal Health Care. NPR. http://www.npr.org/templates/story/story.php?storyId=89651916

Smart Card Alliance. (2005). "The Taiwan Health Care Smart Card Project". http://www.smartcardalliance.org/resources/pdf/Taiwan_Health_Card_Profile.pdf

Statistics Canada (2008) Healthy Canadians: A Federal Report on Comparable Health Indicators 2008

Taiwan Today (March 9, 2010) Health minister resigns over health premium increase. http://www.taiwantoday.tw/ct.asp?xItem=95660&CtNode=414

Tsang IK. Establishing the efficacy of traditional Chinese medicine. Nat Clin Pract Rheumatol 2007;3:60–1.

Tung, Sarah (July 16, 2010). "Is Taiwan Asia's Next One-Stop Plastic-Surgery Shop?". http://www.time.com/time/world/article/0,8599,2004023,00.html#ixzz0u6ep3Q9s

Underwood, Anne (Nov 3, 2009). "Health Care Abroad: Taiwan". The New York Times. http://prescriptions.blogs.nytimes.com/2009/11/03/health-care-abroad-taiwan/?scp=6&sq=hsiao%20taiwan&st=cse

IHS Global Insight

Zuellig Pharma (2006). "The expansion of medical tourism in Asia is proving a healthy boost for a growing number of the region's economies." The Market Partners. Issue 33. pg 8-9.