STATEMENT OF

TONY TRENKLE

DIRECTOR OF THE OFFICE OF INFORMATION SERVICES AND CHIEF INFORMATION OFFICER

CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

REMOVING SOCIAL SECURITY NUMBERS FROM MEDICARE CARDS

BEFORE THE

U.S. HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
AND SUBCOMMITTEE ON HEALTH

AUGUST 1, 2012

Hearing on Removing Social Security Numbers from Medicare Cards

August 1, 2012

Chairmen Johnson and Herger, Ranking Members Becerra and Stark, and distinguished members of the Subcommittees, I am pleased to be here today on behalf of the Centers for Medicare & Medicaid Services (CMS) to discuss the use of Social Security Numbers (SSNs) within Medicare.

CMS takes seriously the risk of identity theft for Medicare beneficiaries. We have removed SSNs from Medicare Summary Notices mailed to beneficiaries on a quarterly basis, and we have prohibited private Medicare health and prescription drug plans from using SSNs on enrollees' insurance cards (e.g., insurance cards for Medicare Advantage, cost contract, and Part D prescription drug plan enrollees). We are engaged in an education effort that provides beneficiaries with information on how to prevent medical identity theft and Medicare fraud. However, the SSN is used as the basis for beneficiary identification because it is fundamental to multiple CMS systems required to process and track beneficiary claims and enrollment, to conduct our antifraud and quality improvement efforts and to coordinate with the Railroad Retirement Board (RRB) and State Medicaid programs across the country.

In response to a request from the House Ways and Means Committee, CMS issued a report in November 2011 entitled *Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards* (November 2011 Update), which examined three different options for removing SSNs from the Medicare card.[1] This report was an update to a 2006 report, *Removal of Social Security Number from the Medicare Health Insurance Card and Other Medicare Correspondence.*[2] As the November 2011 Update described, transitioning to a new identifier would be a task of enormous complexity and cost and one that, undertaken without sufficient planning, would present great risks to continued access to healthcare for Medicare beneficiaries.

[1] Centers for Medicare & Medicaid Services, Report to Congress: Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards. November 2011.
[2] Centers for Medicare & Medicaid Services, Report to Congress: Removal of Social Security Number from the Medicare Health Insurance Card and Other Medicare Correspondence. October 2006.

Social Security Number as Medicare Health Insurance Claim Number (HICN)

From the creation of the Medicare program under the Social Security Act in 1965 until 1977, the Medicare program was administered by the Social Security Administration. While CMS is now responsible for the management of Medicare, the Social Security Administration and Medicare continue to rely on interrelated systems to coordinate both Social Security and Medicare eligibility. Medicare cards include a Health Insurance Claim Number (HICN) which is used as the beneficiary identification number for Medicare. Generally, the HICN is based upon a beneficiary's SSN, or in cases where a beneficiary's Medicare eligibility is based on the employment status and Medicare payroll tax contributions of another person, his or her spouse or parent's SSN. After determining Medicare eligibility, the Social Security Administration transmits the SSN and beneficiary identification code (BIC)[3] to CMS for entry into the CMS Enrollment Database, the data repository for individuals who are or have ever been enrolled in Medicare. CMS then issues the Medicare card with the HICN to the beneficiary. The HICN serves as the primary identifier used for communication between the beneficiary and CMS, and is also used by providers who bill CMS, and for enrollment transactions with Medicare Advantage and prescription drug plans. CMS utilizes the HICN as a beneficiary's identifier in 50 internal CMS systems and in CMS communication with the Social Security Administration, State Medicaid programs, and other nonpayment partners. [4]

When receiving care, the beneficiary shows the provider or supplier their Medicare card with the HICN. The provider or supplier then uses the Medicare card information to check eligibility and to bill Medicare, a process that involves multiple CMS systems. Some examples of the CMS administrative systems that utilize the HICN are: enrollment, quality control, program integrity data for research purposes, and the coordination of benefits. Additionally, the eleven companies contracting with CMS for claims processing communicate with providers or suppliers using the HICN for remittance and payment.

[3] The beneficiary identification code (BIC) is a letter code that appears after the SSN, which corresponds to the relationship of the cardholder to the individual whose work history enables the beneficiary to receive benefits.

[4] Non-payment partners include: States, Railroad Retirement Board, Social Security Administration,, Department of Defense/TriCare, Office of Personnel Management, Department of Veterans Affairs, Indian Health Service, End Stage Renal Disease Networks (REMIS), Department of Treasury (debt referrals), Quality Improvement Organizations and other quality contractors, Program Integrity Contractors, Employers, Federal and State Health Insurance Exchanges (future capability, as permitted by the HIPAA Privacy Rule.)

CMS Reports on the Removal of SSNs from Medicare Cards

CMS appreciates concerns about the ongoing use of SSNs on Medicare cards that have been expressed by beneficiaries and other stakeholders, including Members of Congress. CMS provided an initial examination of the potential challenges and costs posed by the removal of SSNs from Medicare cards in the 2006 report to Congress. In this report, CMS concluded that removing SSNs from Medicare cards would require extensive planning and would be a costly undertaking.

CMS' November 2011 Update provided a current analysis and cost estimate of options for removing SSNs from Medicare cards, as well as three distinct options for removal of SSNs from Medicare cards. Each of the three options evaluated in the November 2011 Update included cost estimates, estimated implementation timeframes, and potential impacts to beneficiaries, providers, insurers, States and other Federal agencies. It identified scenarios related to removal of the SSN from the Medicare card for all current and future Medicare beneficiaries.

CMS found that removing the SSN from Medicare beneficiary identification cards would have immediate and far reaching consequences. As a health care organization, Medicare annually processes about 1.3 billion claims from about 1.5 million providers on behalf of 52 million Medicare beneficiaries. Any change to the Medicare card would impact each Medicare beneficiary, along with health care providers, health insurers and States, as well as the operations and systems of the primary Federal agencies involved in the administration of Medicare–CMS, the SSA, and the Railroad Retirement Board (RRB).

Three Potential Implementation Scenarios Identified

The three scenarios identified in the November 2011 Update each present unique characteristics built around business processes that correlate to different benefits, potential risks and costs. All three implementation scenarios address the concern that the presence of the SSN on the Medicare card presents a risk for identity theft if the card is lost or stolen. As described below, only Scenario 1 replaces the HICN with an entirely new Medicare Beneficiary Identifier (MBI) for purposes of provider billing. As a result, only Scenario 1—the most costly and operationally

challenging of the three options— would allow the MBI used for billing Medicare to be terminated and replaced in the event it was used for fraudulent billing of Medicare.

Scenario One – Medicare Card and Number Replacement/New "MBI"

Under this scenario beneficiaries would receive a new Medicare card with a newly issued MBI, which they would use to receive services from providers. Providers would verify the new MBI and use it for CMS interactions. However, CMS internal systems would process claims and other transactions using the old HICN provided through the use of a translation utility. CMS interfaces with non-payment exchange partners would remain HICN-based, while interfaces with payment partners[5] would use the new MBI. If a beneficiary presented her MBI card to a Government agency such as a SSA Field Office, that agency would convert the MBI to the HICN via a CMS query.

Under this scenario, if an MBI became compromised in some way— for example the number was used for some type of fraudulent purpose—CMS would have the ability to cancel the MBI, issue a new number and card to the Medicare beneficiary, and update its internal utility to use the new data for the MBI to HICN translation.

This scenario would help improve CMS' ability to combat fraud, waste, and abuse since this would provide the ability to turn off an HICN similar to the way credit card companies are able to easily cancel a compromised credit card to stop fraudulent activity and then reissue a new number. Although CMS anticipates there are potential savings associated with an improved ability to turn off or eliminate compromised beneficiary identifiers, CMS cannot determine, at this time, to what extent a new non-SSN beneficiary identifier would more effectively address the problem of compromised identifiers compared to other approaches which identify and combat Medicare fraud currently under development.

Scenario Two - Medicare Card and Number Replacement/New "MBI" for Query Purposes Only

[5] Payment exchange partners: Carriers/MACs/FIs/DME MACs, Providers, DME Suppliers, Part C Plans, Part D Plans

Under this scenario, beneficiaries would receive a new Medicare card with a newly issued MBI. Providers would use the new MBI to query CMS systems to obtain the corresponding old HICN. Unlike Scenario 1 where the providers would use the newly issued MBI to interact with CMS, providers would continue to use the current HICN (based on the SSN) to interact with CMS. CMS internal systems would conduct processing and interface with non-payment and payment exchange partners using the HICN. CMS would use the MBI to interact with beneficiaries. If a beneficiary presented her MBI card to a Government agency such as a SSA Field Office or health care provider, that agency or health care provider would convert the MBI to the HICN via a CMS query.

Scenario 2 would likely place a significant burden on the provider community. In Scenario 2, providers would need to develop the operating procedures and systems capability to: (1) collect a MBI from beneficiaries; (2) electronically request the HICN from Medicare; and (3) then use the HICN for billing purposes.

If the situation warranted, CMS would cancel an existing MBI, issue a new number and card, and update its internal utility to use the new data for the MBI to HICN translation. However, since the HICN remained the beneficiary identifier for billing purposes, CMS would have to use the same types of edits and controls it currently employs in the event a HICN becomes compromised. This scenario maintains the necessity of providers keeping the HICN on file for billing, which would still present a possible risk of identity theft in the event of a data breach in a provider's office.

Scenario Three – Partial HICN Display on Medicare Card

Under the third scenario presented in the November 2011 Update, beneficiaries would receive a new Medicare card with a modified HICN. The change to the Medicare card would be the obscuring of the first five digits of the beneficiary's SSN. This means the BIC portion of the HICN and the last four digits of the SSN would remain visible. Providers would manage verification and eligibility checks through one of the existing resources designed for that purpose. CMS internal systems would continue to conduct processing and interface with non-payment and payment exchange partners using the HICN. However, CMS internal systems,

payment and non-payment exchange partners would require system modifications to accommodate a change to the HICN input fields for verification and eligibility checks.

Since the HICN would remain the beneficiary identifier for billing purposes, CMS would have to use the same types of edits and controls it currently employs in the event a HICN were to become compromised. This scenario would require providers keep the HICN on file for billing, which would still present a possible risk of identity theft in the event of a data breach in a provider's office.

Costs for Implementation

As the Committee requested, the November 2011 Update provided cost estimates for scenarios for removing the SSN from Medicare cards along with the costs and timeframes associated with such options. The SSN-based HICN is the identifier used for 50 CMS systems, as well as for communication with the SSA, RRB, State Medicaid departments and private Medicare health and prescription drug plans. As a result of its widespread use as a foundational component in CMS and partner systems, all the options for changing the beneficiary identifier would be costly, and could require significant changes from the many stakeholders who need to accurately identify the more than 52 million beneficiaries who have Medicare cards with HICNs. In addition, there are substantial costs associated with outreach to those beneficiaries and their providers to ensure any transition goes smoothly, without disruptions in access to care. CMS would be committed to extensive outreach and education for beneficiaries, caregivers, and providers in order to ensure that any transition did not create a new opportunity for fraudsters to take advantage of beneficiary confusion associated with the transition to obtain beneficiaries' personal information.

The November 2011 Update estimated that it would require approximately $812 million to $845 million, depending on the implementation scenario. In general, Scenario 1 is expected to incur the highest costs, primarily based upon the expectation that providers would use the MBI in their interactions with CMS. This would require CMS to modify all systems that receive inquiries and billing transactions from providers to accept the MBI number and immediately interface with the translation utility to replace that with the HICN for internal processing.

Estimates for all three scenarios also considered the projected costs for SSA and RRB,[6] as well as the changes necessary to State Medicaid systems. For beneficiaries dually eligible for Medicare and Medicaid, State Medicaid systems would need to recognize, accept, and transition to the use of a new beneficiary number, as well as incur the cost of matching historical data to the new identifier. In all three scenarios, the cost of converting CMS systems accounts for a significant portion of the cost. These costs include system development costs to cover the planning, gathering, development and implementation of new system changes and include Federal FTE and contractor labor, hardware and software updates for approximately 50 systems. Under all three scenarios, CMS, our Federal partners, and State Medicaid programs would expect to face substantial systems work at a significant cost.

Current CMS Efforts to Prevent Identity Theft

CMS shares the concerns of this Committee and others about the potential identity theft and schemes that target Medicare beneficiaries. Given the budgetary and logistical challenges of removing SSNs from Medicare cards, CMS has already taken a number of steps to protect beneficiaries from identity theft. We have also taken multiple actions to educate beneficiaries about steps they should take to prevent identity theft and fraud, including posting information on the CMS website[7] and adding information to the annual "Medicare & You" Handbook.[8]

Increasing Beneficiary Awareness About Identify Theft

Outreach, education, and ongoing communication are consistently utilized to increase beneficiary awareness about minimizing opportunities for medical identity theft. CMS has a multi-pronged approach to educating beneficiaries and sensitizing them to this important issue that includes the CMS *Medicare & You* handbook and information available online at www.Medicare.gov[9] and www.stopmedicarefraud.gov.[10] Beneficiaries are provided with

[6] SSA and RRB provided estimates of their respective projected costs for all three scenarios.
[7] http://www.medicare.gov/navigation/help-and-support/fraud-and-abuse/fraud-and-abuse-overview.aspx
[8] http://www.medicare.gov/Publications/Pubs/pdf/10050.pdf
[9] Information includes "Protecting Medicare and You from Fraud," which advises beneficiaries on how to protect themselves from identity theft.
[10] Information includes "Medical Identity Theft & Medicare Fraud,", which offers advice on protecting personal information, what to look out for in fraud schemes, how to read Medicare bills, and how to report Medicare fraud or identity theft.

recommendations on who they should provide personal information to and what that information should be. In situations where they are suspicious or concerned about someone requesting personal information, assistance and support contact options are readily available. CMS also encourages our beneficiaries to review their Medicare billing statements and other medical reports in order to spot unusual or questionable charges. On March 7, 2012, Medicare announced the redesign of the quarterly Medicare Summary Notices (MSN) so that beneficiaries can more easily spot potential fraud or irregularities on claims submitted for their care.[11]

CMS has also been partnering with the Administration for Community Living (ACL) to operate the Senior Medicare Patrol program - groups of senior citizen volunteers that educate and empower their peers to identify, prevent, and report identity theft and other forms of health care fraud. The SMP program empowers seniors through increased awareness and understanding of health care programs.

Since the SMP program's inception in 1997, the program has educated over 4.6 million beneficiaries in group or one-on-one counseling sessions and has reached an estimated 27 million people through SMP-led community education outreach events. Over 323,000 Medicare, Medicaid and other complaints of potential health care fraud have been resolved by SMPs or referred for further investigation.

Conclusion

CMS takes seriously our responsibilities to provide high quality health care to beneficiaries while also protecting the privacy of Medicare beneficiaries. CMS has implemented efforts to protect beneficiaries from identity theft through enhanced beneficiary communication, education on identifying and reporting fraud, waste, and abuse, and the importance of protecting Medicare ID numbers. CMS has also taken actions to minimize unnecessary use of SSNs by removing SSNs from Medicare Summary Notices and prohibiting Medicare private health and drug plans from using SSNs on enrollees' insurance cards.

[11] http://www.cms.gov/apps/media/press/release.asp?Counter=4298

CMS appreciates the concerns expressed by Congress and beneficiaries regarding the continued use of SSNs on Medicare cards. However, we recognize that any effort to remove SSNs from Medicare cards would be an administratively complex and costly undertaking, and would require significant advance planning to ensure a smooth transition and appropriate education and outreach.

We pledge to continue our efforts to safeguard beneficiary identification numbers and to maintain dialogue about other options that Congress may wish to consider. I appreciate the Committee's ongoing interest in this issue, and can assure you that CMS is committed to working with Congress to identify ways to best protect beneficiaries' privacy.