STATEMENT OF

SEAN CAVANAUGH

DEPUTY ADMINISTRATOR AND DIRECTOR,
CENTER FOR MEDICARE,
CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

PROTECTING SENIORS FROM IDENTITY THEFT: IS THE FEDERAL GOVERNMENT DOING ENOUGH?

BEFORE THE
U.S. SENATE SPECIAL COMMITTEE ON AGING

OCTOBER 7, 2015

Statement of Sean Cavanaugh on
Protecting Seniors From Identity Theft: Is The Federal Government Doing Enough?
Senate Special Committee on Aging
October 7, 2015

Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for this opportunity to discuss the Centers for Medicare & Medicaid Services' (CMS') work to remove the Social Security Number (SSN) from beneficiaries' Medicare cards. This effort is an important step in protecting beneficiaries from becoming victims of identity theft. Identity theft disrupts lives, damages credit ratings, and can result in inaccuracies on medical records. Medicare fraud wastes taxpayer dollars, and CMS appreciates the Committee's focus on this important topic.

Under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), by April 2019, CMS will eliminate the use of beneficiaries' SSNs as the source of the primary identifier on Medicare cards. CMS has begun the process to redesign Medicare cards by removing the current SSN-based identifier and replacing it with a Medicare Beneficiary Identifier (MBI). For the first time, CMS will be able to terminate a Medicare number as soon as we confirm that is has been compromised and issue a new number to a beneficiary, similar to how credit card companies address stolen card numbers. Being able to immediately deactivate a compromised MBI will enable CMS to quickly respond and better prevent further misuse of a compromised number.

Transitioning to a new MBI will help Medicare beneficiaries better safeguard their personal information by reducing the exposure of their SSNs. This is a complex, multi-year effort that requires both coordination between Federal, state, and private-sector stakeholders as well as an extensive outreach and education program for Medicare beneficiaries, providers, and other stakeholders. CMS will continue our efforts to educate beneficiaries about the risks of medical identity theft, how they can protect their information, and prevent and detect fraud that stems from medical identity theft.

History of Social Security Numbers Within Medicare

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 (SSA). While CMS is now responsible for the management of Medicare, SSA and CMS 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, SSA transmits the SSN and beneficiary identification code (BIC) (the identifying suffix that follows the Medicare number) 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. Often, when receiving care, the beneficiary shows the provider or supplier their Medicare card with the HICN, just as an individual with private insurance uses their insurance card. The provider or supplier then uses the Medicare card information to check eligibility and to bill Medicare, a process that involves multiple CMS systems.

CMS uses the HICN to identify beneficiaries in more than 75 CMS systems, and in CMS communications with other Federal partners. Likewise, providers are required by CMS to use the HICN identifier when they submit claims in order to receive payment for treatments, services, and supplies. CMS and its contractors' systems use the HICN to check for duplicate claims, apply claims and medical policy edits, authorize or deny payment of claims, issue Medicare Summary Notices (MSNs), and conduct printing and mailing operations.

Replacing Health Insurance Claim Numbers with Medicare Beneficiary Identifiers

The initiative to remove SSNs from Medicare cards by replacing HICNs with MBIs is a substantial undertaking. In April 2015, MACRA provided $320 million for this critical initiative. The replacement process will require coordinating with Federal, state, and private sector stakeholders; updating and modifying numerous internal IT systems; and conducting an extensive outreach and education campaign for beneficiaries, providers, and other stakeholders.

CMS is working to accomplish these tasks without disrupting payments to providers, business processes, or beneficiaries' access to care. Taking lessons learned from CMS' implementation of other large-scale, complex IT systems, CMS is developing a thoughtful and measured approach to assure a smooth transition from the first day of use of the MBI.

CMS anticipates that the changes brought about through the shift from HICNs to MBIs will affect more than 75 complex CMS systems, as well as 57 unique State and Territorial eligibility and enrollment and Federal partners' IT systems. For example, SSA and the Railroad Retirement Board (RRB) will need to modify their eligibility and enrollment systems, and the Medicare Administrative Contractors (MACs) and other business partners will need to modify systems to authorize coverage and process claims. Additionally, private insurers and states, including State Medicaid Agencies, will need to modify their systems to process crossover claims.

CMS has been meeting with SSA and RRB to discuss the strategy, timeline, and assumptions for removing the SSN from Medicare cards. CMS will also meet with states and private health plans to coordinate new processes for crossover claims. In addition, CMS has already started the process of procuring a systems integrator to coordinate this multi-faceted project.[1]

CMS will need to develop, test, and execute systems modifications in a way that ensures compatibility with the systems of states, insurers, providers, and every other entity that bills Medicare while avoiding disruption to payment and business processes and beneficiaries' access to care. Once system modifications are in place, issuing new Medicare cards will require an extensive and phased outreach and education program for an estimated 60 million[2] Medicare beneficiaries, as well as providers, private health plans, other insurers, clearinghouses, states, and other stakeholders. We will have a series of communications that will inform beneficiaries that they will be receiving a new card, instruct them on when and how the new card should be used, and inform them how to dispose of their old card. In order to prevent bad actors from taking advantage of potential confusion to gain access to personal information, it will be important to

[1] CMS Small Business Sources Sought, Solicitation Number 160626, https://www.fbo.gov/index?s=opportunity&mode=form&id=baa6a5c5f4d213295219629196f2bd44&tab=core&_cview=0

[2] https://www.cbo.gov/sites/default/files/cbofiles/attachments/44205-2015-03-Medicare.pdf

clearly communicate with our beneficiaries about the timing of and steps necessary to obtain a new card. Additionally, we will have a series of communications to inform Medicare providers of these changes and instruct them on how to use the new identifier to submit claims and other transactions. We must also ensure that private health plans, other insurers, and State Medicaid Agencies are instructed on how to use MBIs so that they can continue their coordination of benefits activities. CMS anticipates that communication activities will begin in January 2018 and continue through April 2019, allowing CMS to meet the deadline established in MACRA.

Working with Beneficiaries to Prevent Medical Identity Theft

The initiative to remove SSNs from Medicare cards will build upon efforts that CMS has already engaged in to protect against identity theft. CMS has already removed SSNs from many types of communications, including MSNs mailed to beneficiaries on a quarterly basis, and we have prohibited private Medicare health (Medicare Advantage) and Prescription Drug (Part D) plans from using SSNs on enrollees' insurance cards (*e.g.*, insurance cards for Medicare Advantage, cost contract, and Part D enrollees).

Beneficiary involvement is a key component of all of CMS' anti-fraud efforts. Alert and vigilant beneficiaries, family members, and caregivers are some of our most valuable partners in stopping fraudulent activity. Information from beneficiaries and other parties helps us to quickly identify potentially fraudulent practices, stop payment to suspect providers and suppliers for inappropriate services or items, and prevent further abuses in the program. CMS has made it easier for beneficiaries to help us fight fraud, waste, and abuse. In 2013, CMS began sending redesigned MSNs,[3] the explanation of benefits for people with Medicare fee-for-service, to make it easier for beneficiaries to spot fraud or errors. The new MSNs include clearer language, descriptions and definitions, and have a dedicated section that tells beneficiaries how to spot potential fraud, waste, and abuse. Beneficiaries are encouraged to report fraud, waste, and abuse to 1-800-MEDICARE, and this is promoted in the re-designed MSN.

CMS engages in a variety of outreach efforts to inform beneficiaries about the risk of medical identity theft and to educate them on steps they can take to protect their personally identifiable

[3] http://blog.medicare.gov/2013/06/06/redesigned-with-you-in-mind-your-medicare-summary-notice/

information. Information is available online and in The Medicare & You handbook, which is distributed to all Medicare households each fall. These resources explain the importance of personal information and how it is used by Medicare; they also include instructions on contacting the appropriate authorities when Medicare fraud, including medical identity theft, is suspected. In these publications, Medicare beneficiaries are advised to take preventive action against identity theft, including:

- Guarding personal information such as Medicare identifiers and SSNs, and only sharing personal information with providers, plans, and suppliers approved by Medicare (a list of approved suppliers is available on Medicare.gov). Importantly, do not give personal information to anyone who calls or comes to the door uninvited, including individuals claiming to be conducting a health survey. Medicare and Medicaid do not send representatives to homes to sell products or services.
- Checking medical bills, MSNs, explanations of benefits, and credit reports for accuracy; use a calendar to record the receipt of services and compare this to Medicare statements.
- Being suspicious of anyone who offers free medical equipment or services; if it is free, they do not need a Medicare number. Do not accept offers of money or gifts for free medical care.
- Not letting anyone borrow or use a Medicare ID card or identity in exchange for goods or services; this is illegal.

CMS has also been partnering with the Administration for Community Living to lend support to the Senior Medicare Patrol (SMP) program, a volunteer-based national program that educates Medicare beneficiaries, their families, and caregivers to prevent, detect, and report Medicare fraud, waste and abuse. The SMP program empowers Medicare beneficiaries through increased awareness and understanding of health care programs and educates them on how to recognize and report fraud. During 2014, SMP program grantees' staff and more than 5,000 volunteers reached over 650,000 people with group education sessions and one-on-one counseling.[4] SMP projects also work to resolve beneficiary complaints of potential fraud in partnership with state and national fraud control and consumer protection entities, including Medicare contractors,

[4] http://www.smpresource.org/Handler.ashx?Item_ID=3A7D6D74-1D4F-4FA6-A8AE-2979022F185F

State Medicaid fraud control units, State attorneys general, the Department of Health and Human Services Office of Inspector General (HHS OIG), and the Federal Trade Commission (FTC).

Addressing Identity Theft and Compromised Numbers

We recognize that despite efforts to safeguard beneficiary information, medical identity theft can still occur. Identity theft complaints from Medicare beneficiaries are received from a number of sources such as calls from beneficiaries and their caregivers to 1-800-MEDICARE, the HHS OIG's Hotline (1-800-HHS-TIPS), our MACs, SMP volunteers, or CMS Regional Offices. CMS has protocols in place to take action when the Agency learns that a beneficiary's number has been compromised. First and foremost, a beneficiary can still receive needed medical care if they have been a victim of identity theft. When a Medicare beneficiary suspects that someone is using their SSN we refer them to the FTC's ID Theft Hotline and the Fraud Hotline of the HHS OIG to file a complaint. In addition, CMS tracks and triages complaints to determine whether the number appears to have been misused, and to ensure that the appropriate corrective actions are taken. If a HICN is compromised, CMS cannot currently issue a new HICN. Once CMS begins issuing MBIs, we will be able to terminate compromised MBIs and issue new beneficiary identification numbers to more immediately mitigate potential fraud.

Currently, if a HICN has been compromised, it is added to our Compromised Numbers Checklist (CNC) database. The CNC is a web-based system that allows direct entry and retrieval of compromised Medicare provider and beneficiary numbers by CMS and CMS contractors. The CNC includes compromised provider and beneficiary numbers obtained through fraud investigations and complaints from providers or beneficiaries. In addition, complaints of identity theft that come into the 1-800-MEDICARE Hotline and CMS contractors (such as Medicare Drug Integrity Contractors, Zone Program Integrity Contractors, or MACs) may be added to the database. For each number, the database includes a specific reason code describing why the number is considered compromised and categorizes the risk as low, medium, or high.

CMS uses the compromised numbers in the CNC database to inform sophisticated analytics through the Fraud Prevention System (FPS). The FPS is an advanced analytics system that identifies and prevents inappropriate payments in Medicare. Through this system, CMS and its

contractors use the CNC data, along with other external data, to identify aberrant and suspicious billing patterns or relationships. Based on the results, CMS focuses its investigative resources on the most egregious behavior. Through the investigations, CMS may provide education or take appropriate administrative action, including revoking a provider's billing privileges, implementing a payment suspension, implementing prepayment edits, requesting an overpayment, or referring the provider to law enforcement.

Moving Forward

Redesigning the Medicare card to remove the SSN-based identifier is a multifaceted initiative that will require complex IT modifications by numerous Federal and state agencies, as well as private partners. It also necessitates significant outreach and education among Medicare beneficiaries and providers. Given how much is at stake, CMS' objectives are to complete the transition to the new cards in a timely fashion that not only improves security, but also minimizes member confusion and disruption from denied claims or access to services. Thank you for your interest in our progress towards removing the SSN from Medicare cards. I look forward to working with the Committee on this important endeavor.