Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

CMS RESPONSE TO BREACHES AND MEDICAL IDENTITY THEFT

Daniel R. Levinson
Inspector General

October 2012
OEI-02-10-00040

CMS RESPONSE TO BREACHES AND MEDICAL IDENTITY THEFT
OEI-02-10-00040

WHY WE DID THIS STUDY

The Centers for Medicare & Medicaid Services (CMS) maintains the protected health information of millions of Medicare beneficiaries. If a breach occurs and the security or privacy of this information is compromised, CMS is required by the American Recovery and Reinvestment Act (the Recovery Act) to notify the affected beneficiaries. Such breaches can lead to medical identity theft. Medical identity theft is the appropriation or misuse of a patient's or a provider's medical identifying information (such as a Medicare identification number) to fraudulently obtain or bill for medical care. It can create patient safety risks and impose financial burdens on those affected. Medical identity theft may also lead to significant financial losses for the Medicare Trust Funds and taxpayers.

HOW WE DID THIS STUDY

We determined the extent to which CMS's response to breaches met the notification requirements in the Recovery Act. We also assessed CMS's response to medical identity theft involving beneficiary and provider Medicare identification numbers and the remedies it offers to beneficiaries and providers. We based this study on CMS data on breaches, CMS policies and procedures, CMS's compromised number database, and structured interviews with CMS staff and benefit integrity contractors.

WHAT WE FOUND

CMS reported that it had 14 breaches of protected health information requiring notification under the Recovery Act between September 23, 2009, and December 31, 2011. CMS notified the 13,775 Medicare beneficiaries affected by the breaches, but did not meet several Recovery Act requirements. CMS has made progress in responding to medical identity theft by developing a compromised number database for contractors. However, the database's usefulness could be improved. Further, contractors do not consistently develop edits to stop payments on compromised numbers. Lastly, CMS offers some remedies to providers but fewer to beneficiaries affected by medical identity theft.

WHAT WE RECOMMEND

We recommend that CMS: (1) ensure that breach notifications meet Recovery Act requirements, (2) improve the compromised number database, (3) provide guidance to contractors about using database information and implementing edits, (4) develop a method for ensuring that beneficiaries who are victims of medical identity theft retain access to needed services, and (5) develop a method for reissuing identification numbers to beneficiaries affected by medical identity theft. CMS concurred with all but the draft report's fourth recommendation, which we revised as stated above.

TABLE OF CONTENTS

OBJECTIVES

1. To determine the extent to which the Centers for Medicare & Medicaid Services' (CMS) response to breaches of beneficiaries' protected health information met the notification requirements in the American Recovery and Reinvestment Act of 2009 (the Recovery Act).
2. To assess CMS's response to medical identity theft involving beneficiary and provider Medicare identification numbers and the remedies it offers to beneficiaries and providers.

BACKGROUND

CMS maintains the protected health information of millions of Medicare beneficiaries, storing, receiving, and transmitting it daily.[1] If CMS has a breach of unsecured (or unencrypted) protected health information, it is required by the Recovery Act to notify the affected beneficiaries.[2] A breach is defined by the Recovery Act as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[3] Breaches of health information can lead to medical identity theft.

Medical identity theft is the appropriation or misuse of a patient's or a provider's medical identifying information (such as a Medicare identification number) to fraudulently obtain or bill for medical care, prescription drugs, or supplies. It can affect beneficiaries or providers. Such theft can create patient safety risks and impose financial burdens on those affected. It can lead to erroneous entries in beneficiaries' medical histories and even to the wrong medical treatment. Medical identity theft may also lead to significant financial losses for the Medicare Trust Funds and taxpayers.

In previous reports, the Office of Inspector General (OIG) and the Government Accountability Office (GAO) identified gaps and weaknesses

[1] The phrase "protected health information" is defined by regulation to mean, with some exceptions, identifying information created or received by an employer or a health care entity that relates to an individual's physical or mental health condition and is transmitted or maintained in any medium. See 45 CFR § 160.103.

[2] While CMS also maintains the health information of Medicaid beneficiaries, which is subject to Recovery Act breach notification requirements, this report is limited to breaches of Medicare information.

[3] The Recovery Act, P.L. 111-5 § 13400(1). Title XIII of the Recovery Act is also referred to as the Health Information Technology for Economic and Clinical Health Act, or the HITECH Act. The Department of Health and Human Services (HHS) implemented the breach notification requirements at 45 CFR Pt. 164, subpart D.

in the information security procedures of CMS and its contractors.[4] To date, no evaluation has examined CMS's breach notification procedures or determined how many breaches involving beneficiaries' protected health information have occurred. There has also been no evaluation of CMS's efforts to respond to medical identity theft involving Medicare beneficiary or provider identification numbers.

Breach Notification

The Recovery Act requires covered entities—such as health care providers and plans—and their business associates to notify an individual whose unsecured protected health information[5] has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach.[6] An example of a breach that would require notification under the Recovery Act is the loss of a CMS laptop containing unencrypted Medicare beneficiary identification numbers.

The Recovery Act requirements became effective on September 23, 2009.[7] As a covered entity, CMS is subject to these requirements.[8] CMS's contractors are considered business associates[9] and are required to inform CMS of any breaches and provide the information necessary for CMS to make the required notifications to affected individuals.[10]

The notification requirements pertain to breaches of beneficiaries' protected health information; provider Medicare identification numbers are not covered by the Recovery Act notification requirements. These numbers are not "protected health information" because they do not relate to the provider's health status.

The Recovery Act requires that notification to each affected individual include:

- a description of what happened, including the dates of both the breach and its discovery, if known;
- the type(s) of unsecured protected health information involved;

---

[4] OIG, *Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2009*, A-18-10-30300, September 2011. GAO, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267, February 2006.

[5] Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals using methods approved by the Secretary.

[6] The Recovery Act §§ 13402 and 13404; see also 45 CFR §§ 164.404(a) and 164.410.

[7] 74 Fed. Reg. 42740 (Aug. 24, 2009). Publication of the final rule is pending.

[8] 45 CFR § 160.103; CMS Program Memorandum, Transmittal AB-03-034 (February 28, 2003).

[9] CMS Program Memorandum, Transmittal AB-03-034 (February 28, 2003).

[10] The Recovery Act § 13402(b); 45 CFR § 164.410.

- steps individuals should take to protect themselves from potential harm;
- a description of how the covered entity is investigating the breach, mitigating losses, and protecting against further breaches; and
- contact procedures for individuals who want to learn more.[11]

In general, affected individuals must be notified by first-class mail, "without unreasonable delay," and no more than 60 days after the breach has been discovered.[12]

In addition, covered entities must notify HHS of any breaches not later than 60 days after the end of the calendar year during which the breach occurred.[13] HHS must in turn identify the covered entity involved in the breach on its Web site.[14] If any breach affects 500 or more residents of a State or jurisdiction, the covered entity must also notify prominent media outlets in the area.[15] The notification to media outlets must contain the same information as the notification to individuals.[16] In these cases, notification must also be provided to HHS contemporaneously with individual notification.[17]

Medical Identity Theft

Breaches may lead to medical identity theft. Medical identity theft is the misuse of provider or beneficiary medical identifying information. An example of medical identity theft occurs when someone obtains unencrypted Medicare identification numbers of beneficiaries and uses them to submit false claims to CMS. This is against Federal law, which prohibits using another person's identification to make false statements when seeking payment under a Federal health care program.[18]

CMS Contractors

CMS relies on contractors to review and pay claims. These contractors maintain the protected health information of Medicare beneficiaries as part of their duties. As business associates of CMS, they are required by the Recovery Act to inform the agency if they commit any breaches of this information. They are also involved in CMS's efforts to identify and

[11] The Recovery Act § 13402(f); 45 CFR § 164.404(c).
[12] The Recovery Act §§ 13402(d)(1) and 13402(e)(1); 45 CFR § 164.404. Section 13402(g) of the Recovery Act allows for a delay of notification for law enforcement purposes.
[13] The Recovery Act § 13402(e)(3); 45 CFR § 164.408(c).
[14] The Recovery Act § 13402(e)(4).
[15] The Recovery Act § 13402(e)(2); 45 CFR § 164.406(a).
[16] 45 CFR § 164.406(c).
[17] 45 CFR § 164.408.
[18] 18 U.S.C. § 1028A(a) and 42 U.S.C. § 1320a–7b.

respond to medical identity theft involving Medicare beneficiary or provider information.

Contractors have a range of duties. Zone Program Integrity Contractors (ZPIC) conduct Part A- and Part B-related benefit integrity activities.[19] They recommend claims processing edits to suspend or deny potentially improper payments, including those that result from medical identity theft. They are also responsible for identifying and investigating potential fraud.

Medicare Drug Integrity Contractors (MEDIC) conduct Part C- and Part D-related benefit integrity activities.[20] Their work includes analyzing Part D prescription claims data and reviewing beneficiary complaints to prevent the payment of fraudulent claims. They recommend appropriate administrative actions to CMS, which may include denying or recouping fraudulent payments. Hereinafter, we refer to the MEDICs and ZPICs collectively as "benefit integrity contractors."

Compromised Number Database

CMS's compromised number database, first released in February 2010, contains beneficiaries' and providers' Medicare identification numbers that have been involved in, or are suspected of having been involved in, medical identity theft and those that are vulnerable to medical identity theft. Medicare identification numbers of beneficiaries are also known as Health Insurance Claim numbers. In this report, we refer to Medicare identification numbers of beneficiaries as "beneficiary numbers." Medicare identification numbers of providers are also known as National Provider Identifiers. In this report, we refer to Medicare identification numbers of providers as "provider numbers."

METHODOLOGY

This study is based on several data sources: (1) CMS data on breaches, (2) CMS breach policies and procedures, (3) CMS's compromised number database, and (4) structured interviews with CMS staff and benefit integrity contractors.

Review of CMS Data on Breaches

We requested data from CMS on the number of breaches that occurred between September 23, 2009 (when the Recovery Act notification requirements became effective), and December 31, 2011. We considered a breach committed by CMS or by any of CMS's contractors acting in their

[19] ZPICs are assuming the role formerly held by Program Safeguard Contractors. Five ZPICs were operating and two zones were transitioning at the time of our review.

[20] One MEDIC focuses on benefit integrity and its work consists primarily of claims analysis and investigations. The other MEDIC handles compliance and enforcement issues.

capacity as business associates to be a CMS breach. We analyzed the data to enumerate and describe the breaches known by CMS to have occurred within the specified time period.

Review of CMS Policies and Procedures Regarding Breaches

We requested from CMS its policies and procedures for responding to breaches. We also requested documentation on how CMS responded to breaches that occurred after the Recovery Act went into effect, September 23, 2009, through December 31, 2011. This documentation included the notifications CMS provided to affected individuals.

We reviewed CMS's policies and procedures to determine how CMS responds to breaches. We also reviewed the notifications CMS provided to affected individuals to determine the extent to which CMS met Recovery Act requirements. We determined whether the notifications included a description of what happened, including the dates of both the breach and its discovery; the type(s) of unsecured protected health information involved; steps individuals should take to protect themselves from potential harm; a description of how the covered entity is investigating the breach, mitigating losses, and protecting against further breaches; and contact procedures for individuals who want to learn more. We also determined whether CMS provided the notifications within 60 days of the breaches' discovery, as required by the Recovery Act.

Review of Database Containing Compromised Medicare Identification Numbers

We requested and analyzed the database of compromised beneficiary and provider numbers that CMS maintains. We reviewed the February 2012 version of the database.

Structured Interviews With CMS Staff and Benefit Integrity Contractors

We conducted structured interviews with key CMS staff responsible for developing and implementing policies and procedures regarding breaches and medical identity theft. We asked how CMS identifies and responds to breaches and instances of medical identity theft, including what remedies are available for affected beneficiaries and providers.

In addition, we interviewed staff from CMS's benefit integrity contractors (five ZPICs that were operating at the time of our review and the two MEDICs). We asked them how they identify and respond to instances of medical identity theft involving Medicare identification numbers. We also asked how they use CMS's compromised number database. Further, we inquired about remedies available to beneficiaries and providers affected by medical identity theft.

Limitations

This study was limited to breaches known to CMS that required notification under the Recovery Act. The findings are based on an analysis of CMS data. We did not independently determine whether there were additional breaches.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

CMS had 14 breaches requiring notification under the Recovery Act

Over a 2-year period, between September 23, 2009, and December 31, 2011, CMS had 14 breaches that, by its own determination, required notification of the affected individuals under the Recovery Act. As a covered entity, CMS must provide notification if it reasonably believes the information has been accessed, acquired, used, or disclosed as a result of a breach.[21] CMS considers several factors when making this determination, including the nature of the data elements breached and the likelihood that the information is accessible and usable.

In general, CMS's breaches involved beneficiaries' names, Medicare identification numbers, dates of birth, diagnoses, and services received. In total, 13,775 Medicare beneficiaries were affected by the 14 breaches requiring notification. One breach affected 13,412 beneficiaries. This breach involved a Medicare Summary Notice printing error by a CMS contractor, which caused the notices to be sent to incorrect addresses. Ten breaches resulted from other mismailing or from loss of documents during transit. In another two breaches, beneficiary information was posted online. In the remaining breach, a CMS contractor employee was arrested for stealing beneficiary information. See Table 1 for more details about the 14 breaches.

Table 1: Breaches Requiring Notification, Reported by CMS (From September 23, 2009, Through December 31, 2011)

Type of Breach	Number of Breaches	Number of Affected Beneficiaries
Medicare Summary Notice printing error	1	13,412
Beneficiary information posted online	2	190
Mismailings or loss during transit	10	165
Stolen beneficiary information	1	8
Total	**14**	**13,775**

Source: OIG analysis of CMS data on breaches requiring notification under the Recovery Act, 2012.

[21] 45 CFR § 164.404(a).

CMS notified beneficiaries of the breaches, but did not meet several Recovery Act requirements

Although CMS notified all beneficiaries affected by the 14 breaches, it failed to meet the Recovery Act's standard for timeliness for 7 of them. Notification letters for these breaches were not sent to the beneficiaries within the timeframe dictated by the Recovery Act (without unreasonable delay and in no case later than 60 days after the date of discovery).[22] Notifications for some breaches were sent 4 days after the 60-day timeframe, while others were sent more than 4 months after the 60 days. Notification letters for the largest breach were sent within the required timeframe.

The notifications for these breaches often were missing required information. Notably, the notification letters for six of the breaches did not explain how the contractors were investigating the breach, mitigating losses, or protecting against further breaches, as required by the Recovery Act. Moreover, notification letters for half the breaches, including the largest breach, were missing either the date the breach occurred or the date it was discovered. Notification letters for three breaches did not include the types of unsecured protected health information involved, contact procedures for individuals who want to learn more, or steps individuals can take to protect themselves from harm. See Table 2.

Table 2: CMS Breaches and Recovery Act Notification Requirements

Recovery Act Notification Requirement	Number of Breaches Not Meeting Requirement
Notification within 60 days of breach's discovery	7
Description of breach investigation, loss mitigation, and protection against further breaches	6
Date breach occurred or was discovered	7
Information involved, contact procedures, or steps to protect from harm	3

Source: OIG analysis of CMS data on breaches requiring notification under the Recovery Act, 2012.

CMS informed HHS of all 14 breaches within the required timeframes. In addition, CMS provided timely notice to the media for the largest breach, as required for breaches affecting 500 or more residents of a State or jurisdiction. Although this breach affected individuals in 9 States, the impact was concentrated in Tennessee, which was home to over 13,000 of

[22] 45 CFR §§ 164.404(b) and 164.410(b).

the affected individuals. Accordingly, CMS notified media outlets in Tennessee only. HHS also posted notice of the breach on its Web site. However, the media notification regarding this breach neglected to include steps that individuals should take to protect themselves from harm.

CMS has made progress in responding to medical identity theft by developing a compromised number database for contractors

Medical identity theft is the misuse of medical identifying information, such as beneficiary numbers and provider numbers, to fraudulently obtain or bill for medical services or supplies. CMS's response to medical identity theft has centered on maintaining a database of compromised beneficiary and provider numbers. The database contains numbers that have been involved in, or are suspected of having been involved in, medical identity theft and those that are vulnerable to medical identity theft. As of February 2012, the database contained the Medicare numbers of almost 284,000 beneficiaries and 5,000 providers. The database also includes classifications that indicate the level of risk associated with each compromised number. Numbers are classified as high, medium, or low risk.[23] The majority of the numbers in the database were classified as medium risk. See Table 3 for a summary of the risk-level information in the database.

Table 3: Compromised Numbers as Reported by CMS, by Risk Level

Risk Level	Medicare Beneficiaries	Medicare Providers
High	56,164	1,383
Medium	213,792	3,547
Low	13,616	32
Total	**283,572**	**4,962**

Source: OIG analysis of CMS compromised number database, February 2012 version.

The beneficiary and provider numbers in the database come from CMS's benefit integrity contractors. These contractors identify the numbers

[23] High-risk numbers have been confirmed as compromised. For instance, a beneficiary number is considered high risk if at least one inappropriate service was billed with it. Numbers categorized as low risk have been identified as potentially compromised. For instance, a beneficiary number is considered low risk if the beneficiary reported the loss of his or her Medicare card. Medium-risk numbers are strongly suspected of having been compromised.

through claims analysis and complaint investigations and send them to CMS monthly.[24] CMS consolidates this information into a database and sends it to each contractor on a compact disk once a month. CMS also incorporates the database into its predictive modeling initiative.[25] The goal of this initiative is to identify unusual billing activity and establish risk scores to identify claims for review before payment is made.

Opportunities exist for improving the database's usefulness

CMS has provided benefit integrity contractors with technical guidance about how to submit beneficiary and provider numbers and additional information to the compromised number database. However, CMS has not issued guidance to contractors about how to incorporate database information into their benefit integrity activities.

As a result, benefit integrity contractors use the database in different ways. Some contractors use it to discover numbers that they did not know were compromised. These contractors routinely compare all the compromised numbers in the database to the beneficiary and provider numbers on claims that have been submitted in their area. In contrast, one contractor compares only beneficiary and provider numbers it is investigating to numbers in the database. In both cases, if contractors find a match, they investigate further.

Further, benefit integrity contractors rarely use information in the database other than the numbers. In fact, one contractor was not aware that the database contained other information, such as the date the number was added to the database or edits associated with the number.

Benefit integrity contractors also noted that information can be difficult to find in the database. For example, a field in the database that is supposed to contain the reason that numbers were added to the database was blank for 75 percent of the high-risk beneficiary numbers and 62 percent of high-risk provider numbers. Knowing the reason a number is considered compromised can assist contractors in their investigations.

Some contractors characterized the database as not user friendly. They described the interface as cumbersome and ill-suited to the database's high volume of information. One contractor noted that the database seems to have been designed to facilitate investigations of individual cases, whereas benefit integrity contractors focus on large-scale data analysis.

---

[24] All ZPICs are required to report information for the database. The benefit integrity MEDIC began doing so in July 2010. The compliance and enforcement MEDIC is not required to report information for inclusion in the database.

[25] This initiative grew out of legislation that required CMS to use predictive modeling. See Small Business Jobs Act of 2010, P.L. 111-240 § 4241; 42 U.S.C. § 1320a-7m.

Contractors also commonly noted that the database does not meet their need for up-to-date data. Several said that they would like the database to be available in real time, instead of being distributed monthly.

In addition, some contractors have concerns about the quality of the information in the database. These contractors noted that they place minimal weight on database information mainly because they believe that other contractors' standards for categorizing numbers differ from their own.

CMS contractors do not consistently develop edits to stop payments on compromised numbers

Most benefit integrity contractors cited claims processing edits as a powerful tool against medical identity theft. When a contractor develops an edit for a compromised beneficiary or provider number, the contractor can deny claims that contain that number or identify claims for further scrutiny.[26]

Contractors vary in the extent to which they develop edits for compromised numbers. They also differ in the types of edits that they develop. One contractor focused its edits exclusively on provider numbers. This contractor did not develop edits for beneficiary numbers at all. In contrast, other contractors noted that they routinely develop edits for individual beneficiary numbers. Another contractor developed only autodenial edits, which automatically deny claims using predetermined criteria. Other contractors make extensive use of prepay edits, which identify claims for individual review prior to payment.

Contractors reported that they consider potential consequences when deciding whether to develop edits. For instance, contractors do not want to limit access to needed services for a beneficiary whose number has been stolen. Taking this into account, a contractor may put edits in place for certain types of services, such as durable medical equipment, but may allow other services, such as emergency room visits. Another consequence is that edits can conflict with criminal investigations, as payment delays and claim denials can tip off fraudulent billers. Law enforcement agencies might request that contractors refrain from developing an edit so that law enforcement can track claims and build a criminal case. In these instances, contractors can work with law enforcement to come to an agreement on when to stop claim payments.

[26] For Medicare Part C and Part D, private plans are responsible for developing and implementing edits.

CMS offers some remedies to providers but fewer to beneficiaries affected by medical identity theft

Providers and beneficiaries affected by medical identity theft are susceptible to adverse financial and Medicare benefit-related consequences if their numbers are misused. For example, providers can be subject to tax liabilities and requests for reimbursement of Medicare payments for claims that they did not submit. For beneficiaries, claims resulting from the misuse of their numbers may count toward Medicare caps that limit services and medical devices that they are eligible to receive. For instance, outpatient therapy is subject to Medicare benefit caps.[27]

CMS has taken some steps to assist providers affected by medical identity theft

CMS has implemented a Provider Victim Validation/Remediation Initiative, which establishes protocols for assisting legitimate providers who have incurred Medicare financial liabilities, such as overpayment demands and tax liabilities, because of identity theft. Such situations can occur, for example, if an individual with access to provider information fraudulently bills Medicare and redirects Medicare payments to himself or herself.

Providers who have suffered financial liabilities are told to contact benefit integrity contractors. The contractors conduct investigations and send the results to CMS. CMS then decides whether to relieve the providers of the liabilities. Another remedy available to providers is the assignment of new Medicare identification numbers.

CMS offers few remedies for beneficiaries affected by medical identity theft

Medicare beneficiaries who suspect fraud or identity theft are encouraged to call the 1-800-MEDICARE hotline.[28] Hotline representatives refer suspected fraud to a benefit integrity contractor for further investigation. The contractor determines whether the beneficiary number should be added to the compromised number database. According to CMS officials, the contractor must acknowledge to the beneficiary that the complaint was

[27] CMS, *Medicare Claims Processing Manual*, Pub. No. 100-04, ch. 5, § 10.2.

[28] CMS, *Protecting Medicare and You from Fraud*, Pub. No. 10111, October 2011, p. 5. Accessed at https://www.medicare.gov/Publications/Pubs/pdf/10111.pdf on June 21, 2012. Also, OIG has created a brochure containing tips on how to avoid medical identity theft and instructions for reporting Medicare fraud and medical identity theft. Accessed at http://oig.hhs.gov/fraud/medical-id-theft/OIG_Medical_Identity_Theft_Brochure.pdf on June 21, 2012.

received but does not provide details to beneficiaries when a case is under investigation.

Beneficiaries with compromised numbers are not routinely assigned new numbers. Several benefit integrity contractors expressed a desire for CMS to terminate and issue new beneficiary numbers, citing the credit card industry as a model. According to most contractors, new beneficiary numbers would minimize the damage caused by medical identity theft. One contractor noted that assigning new numbers would greatly assist beneficiaries because resolving issues associated with a compromised number can be time consuming and financially draining for the beneficiaries.

One obstacle to assigning new numbers is that beneficiary numbers are linked to Social Security numbers. The Social Security Administration OIG has encouraged CMS to eliminate Social Security numbers from beneficiaries' Medicare numbers.[29] CMS officials, however, have cited high costs, the volume of changes, and operational and systems issues as barriers to altering beneficiary numbers.[30]

Further, there is no standard procedure for ensuring that beneficiaries retain their access to services if their Medicare numbers have been misused by others. If a beneficiary's number is misused, a claim for a service or an item resulting from the misuse is included in the beneficiary's Medicare billing history. This could delay or prevent beneficiaries from receiving needed services, particularly when these services are subject to a cap.

[29] Social Security Administration OIG, *Removing Social Security Numbers from Medicare Cards*, A-08-08-18026, May 2008.

[30] Part C and Part D plans generate their own identification numbers for enrollees that are different from the Social Security numbers.

CONCLUSION AND RECOMMENDATIONS

As the single largest health care payer in the United States, CMS plays a critical role in addressing breaches of protected health information and medical identity theft. Breaches and medical identity theft put beneficiaries, providers, and the Medicare Trust Funds at risk. If CMS does not follow the requirements for handling breaches, opportunities increase for medical identity theft and fraudulent billing of the Medicare program.

CMS reported that it had 14 breaches requiring notification under the Recovery Act between September 23, 2009, and December 31, 2011. CMS notified the 13,775 beneficiaries affected by the breaches, but did not meet several Recovery Act requirements.

CMS has made progress in responding to medical identity theft by developing a compromised number database for contractors. However, the database's usefulness could be improved. CMS has not issued guidance to contractors about how to incorporate database information into their benefit integrity activities, and as a result, contractors use the database in different ways. Also, contractors do not consistently develop edits to stop payments on compromised numbers. Lastly, CMS offers some remedies to providers but fewer to beneficiaries affected by medical identity theft.

We recommend that CMS:

Ensure That Breach Notifications Meet Recovery Act Requirements

CMS should ensure that breach notifications are sent within the required timeframe and include the required information. Notifications must include a description of how CMS is investigating the breach, mitigating losses, and protecting against further breaches. They must also include a description of what happened, the type of information involved, steps individuals should take to protect themselves, and contact procedures for individuals who want to learn more.

Improve the Compromised Number Database

CMS should solicit input from the benefit integrity contractors and improve the completeness and quality of the database. CMS should also make the database more user friendly, moving away from monthly mailings to a system that would allow for timelier reporting and access. Improving the database would enable contractors to use it more extensively to better detect and deter medical identity theft.

Provide Guidance to Contractors About Using Database Information and Implementing Edits

We recognize that CMS uses database information in its predictive modeling initiative. In addition, CMS should provide guidance to contractors about how to incorporate database information into their benefit integrity activities. CMS should also provide contractors with protocols for developing edits for compromised numbers. These protocols should outline the circumstances that warrant edits and the types of edits that are most appropriate for compromised provider and beneficiary numbers. These protocols could help promote consistent use of edits across contractors.

Develop a Method for Ensuring That Beneficiaries Who Are Victims of Medical Identity Theft Retain Access to Needed Services

CMS should mitigate the damage of medical identity theft by ensuring that beneficiaries retain their access to services if their Medicare numbers have been misused by others. Misuse of a beneficiary's number could delay or prevent that beneficiary from receiving needed services, particularly when the services are subject to a cap. CMS could insert an indicator in the beneficiary claim record that would exclude certain claims from frequency and utilization edits, allowing for payment of legitimate claims for victims of medical identity theft. CMS could also develop other methods for providing assurances and documentation to these beneficiaries that their access to services will not be restricted as a consequence of the theft.

Develop a Method for Reissuing Identification Numbers to Beneficiaries Affected by Medical Identity Theft

The issuance of new Medicare beneficiary numbers is complex. We recognize that there is no easy solution to this problem, given that beneficiaries' Medicare numbers currently are linked to their Social Security numbers. However, CMS should explore different options and then develop a method for reissuing Medicare numbers to beneficiaries affected by medical identity theft.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS concurred with four of the five recommendations in the draft report. With regard to the first recommendation, CMS concurred and stated that it will develop new procedures and/or modify existing ones to improve the breach notification process. With regard to the second recommendation, CMS concurred and is working with system users to both identify improvements to design a more user-friendly database and add critical information about each compromised number to support fraud detection efforts. CMS is also developing a Web-based interface that will allow direct access by users. CMS also concurred with our third recommendation and stated that it has issued instructions and guidance to contractors regarding updating, entering, and redefining entries in the database. Also, CMS intends to share edit development best practices for compromised numbers and issue edit development protocols.

CMS did not concur with the fourth recommendation in the draft report to correct beneficiary billing histories. CMS cited concerns that changing billing records could negatively impact criminal and civil prosecutions and the integrity of the Medicare claims processing system. However, CMS stated that it will consider the insertion of an indicator on the beneficiary claim record that would allow for payment of legitimate claims for victims of medical identity theft. In response, we modified the fourth recommendation to include CMS's comments and to focus on developing a method for ensuring that beneficiaries who are victims of medical identity theft retain access to needed services.

Finally, CMS concurred with the fifth recommendation and noted that making the necessary changes to allow CMS to reissue identification numbers for beneficiaries will require significant monetary investments and multiple systems and operational changes for CMS, its contractors, the Social Security Administration, State Medicaid programs, private health plans, and providers. CMS stated it is reviewing options and cost estimates for developing an identification number that is not based on the Social Security number.

The full text of CMS’s comments is provided in the appendix.

APPENDIX

Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: AUG 2 7 2012

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner /S/
Acting Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "CMS Response to Breaches and Medical Identity Theft" (OEI-02-10-000040)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the OIG Draft Report entitled, "CMS Response to Breaches and Medical Identity Theft" (OEI-02-10-000040). The objectives of this study are to determine the extent to which CMS' response to breaches of beneficiaries' protected health information met the notification requirements in the American Recovery and Reinvestment Act of 2009 (the Recovery Act) and to assess CMS's response to medical identity theft involving beneficiary and provider Medicare identification numbers, as well as the remedies it offers to beneficiaries and providers.

The OIG examined the 14 breaches requiring notification under the Recovery Act between September 23, 2009 and December 31, 2011. The report indicates that CMS did notify the 13,775 Medicare beneficiaries affected by the breaches, but did not meet several Recovery Act requirements. OIG also reports that CMS has made progress in responding to medical identity theft by developing a compromised number database for contractors, but improvements are needed to increase database utility and improve edit development designed to stop payments. Lastly, OIG acknowledges that CMS offers some remedies to providers but fewer to beneficiaries affected by medical identity theft.

The CMS appreciates OIG's efforts in working with our agency to help ensure that health information of Medicare beneficiaries is protected. CMS' response to each of the OIG recommendations follows.

OIG Recommendation 1

The CMS should ensure that breach notifications meet Recovery Act Requirements.

CMS Response

The CMS concurs with this recommendation. Our policy and procedures reflect the Recovery Act's breach notification provisions. To ensure breach notifications are sent within the required

timeframe and include the required information, we will initiate an analysis of the agency's current incident handling process to identify gaps and to strategize action(s) for improvement. Based on these findings, we will develop new procedures and/or modify existing ones to improve the process, resulting in more efficient breach response.

OIG Recommendation 2

The CMS should improve the Compromised Number Database.

CMS Response

The CMS concurs with this recommendation. CMS is in the process of improving the completeness, quality, and accessibility of the Compromised Number Checklist (CNC) database. CMS is currently working with system users (e.g., ZPICs, PSCs, MEDIC, OIG Office of Investigations and the Federal Bureau of Investigation) to both identify improvements to design a more user-friendly database and add critical information about each compromised number to support fraud detection efforts. CMS plans to complete this quality improvement in 2012. CMS is also developing a web-based interface for the CNC that will allow direct access by users (CMS staff and contractors and law enforcement). Once the enhanced CNC system is launched, system users will have the capability to directly search, view, enter and update compromised number records in the national database. CMS plans to complete the enhancement of the CNC database in the first quarter of 2013.

OIG Recommendation 3

The CMS should provide guidance to contractors about using database information and implementing edits.

CMS Response

The CMS concurs with this recommendation. CMS has issued instructions via teleconferences and written guidance such as the recent Technical Direction Letters to the PSCs/ZPICs and MEDICs regarding updating, entering and redefining the entries in Compromised Number Checklist (CNC) database. The purpose of CPI's guidance is to increase consistency and efficiency in usage of the database. Several PSCs/ZPICs have developed edits for compromised numbers. Once the CNC redefinition project has been completed, CPI intends to share edit development best practices for compromised numbers across the PSCs/ZPICs and use that information and experience as the basis for development and issuance of edit development protocols.

OIG Recommendation 4

The CMS should develop protocols for correcting beneficiary billing histories.

CMS Response

The CMS does not concur with this recommendation. Our major concern is that CMS' adjustment of beneficiary billing records could have a negative impact on criminal and civil prosecutions and on the underlying integrity of the Medicare claims processing system. If Trust Fund dollars were paid, adjusting beneficiary history to reflect otherwise (in the absence of established processes such as claim denials resulting from post pay review), could have damaging effects on beneficiaries' deductible and coinsurance status and on the accuracy of CMS' internal accounting systems such as Healthcare Integrated General Ledger Accounting System. It seems questionable whether an United States Assistant Attorney would indict and prosecute cases in which CMS has adjusted beneficiary billing histories. CMS recommends that OIG-OEI discuss the implications of its beneficiary history correction recommendation with its Office of Investigations and the Department of Justice.

The CMS will consider the insertion of an indicator in the beneficiary claim record which would exclude certain claims from future frequency and utilization driven edits to allow payment of legitimate claims for beneficiaries victimized by identity theft.

OIG Recommendation 5

The CMS should develop a method for reissuing identification numbers for beneficiaries who are affected by medical identity theft.

CMS Response

CMS concurs with the OIG's recommendation to explore different options for a beneficiary identifier that would allow CMS to reissue identification numbers for beneficiaries who are affected by medical identity theft. As the OIG notes, currently the Social Security Administration (SSA) assigns the Medicare beneficiary identifier- the Health Insurance Claim Number (HICN) - which is based on an individual's or the individual's spouse's Social Security Number. Furthermore, the SSA is the only entity that can assign a new Social Security Number (SSN) or HICN to an individual. Thus, CMS cannot terminate HICNs and reissue new non-Social Security based numbers, even to Medicare beneficiaries who are victims of identity theft.

Making the necessary changes to allow CMS to reissue identification numbers for beneficiaries will require significant monetary investments, multiple systems and operational changes, not just for CMS and its contractors, but also for SSA, state Medicaid programs, private health plans and providers that CMS interacts with regarding beneficiary information for enrollment and claims payment. However, we recognize the importance of finding ways to better protect personally identifiable information for beneficiaries and to assist beneficiaries who are victims of medical identity theft. Furthermore, CMS is currently examining ways to further safeguard Medicare numbers in communications with beneficiaries for the purpose of lowering the risk of compromising this information. In addition, CMS is reviewing options and cost estimates for a non-SSN-based identification number for Medicare beneficiaries that would enable CMS to re-issue a compromised Medicare number.

Again, we appreciate the opportunity to comment on this draft report and look forward to working with OIG on this and other issues.

ACKNOWLEDGMENTS

This report was prepared under the direction of Jodi Nudelman, Regional Inspector General for Evaluation and Inspections in the New York regional office.

Deputy Regional Inspector General Nancy Harrison served as the team leader for this study. Other Office of Evaluation and Inspections staff from the New York regional office who conducted the study include Rose Goldberg, Olivia Herman, Jennifer Karr, and Michael Rubin. Central office staff who provided support include Scott Horning, Kevin Manley, Debra Roush, Tasha Trusty, and Rita Wurm.

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.