Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

DISCLOSURE AND ACCOUNTING OF PROTECTED RECORDS BY CMS BETWEEN 2006 AND 2011

Daniel R. Levinson
Inspector General

January 2014
OEI-09-11-00430

EXECUTIVE SUMMARY: Disclosure and Accounting of Protected Records by CMS Between 2006 and 2011
OEI-09-11-00430

WHY WE DID THIS STUDY

The Centers for Medicare & Medicaid Services (CMS) maintains millions of records containing financial and health-related information. Inappropriate disclosures of records or data maintained in a system of records (SOR) can result in loss of privacy and fraudulent activities. The Privacy Act of 1974 (Privacy Act) governs Federal agencies' collection, use, and dissemination of individuals' records maintained in an SOR. CMS maintains SORs, and its disclosures of records must be consistent with the Privacy Act. Further, the Privacy Act requires CMS to implement safeguards that protect records maintained in an SOR and to account for any disclosures. Among other things, CMS uses a data use agreement (DUA) to ensure its disclosures are in compliance with the Privacy Act. A DUA is the legally binding agreement that contains the written terms and conditions that govern each disclosure. Entities are required to submit a DUA and DUA-related documents to CMS prior to the disclosures.

HOW WE DID THIS STUDY

We reviewed data requests approved or renewed by CMS between September 2006 and August 2011. We limited our review to approved data requests from health-related SORs. We used the DUA tracking number generated by the Data Agreement and Data Shipping Tracking System (DADSS) to identify our population of approved requests. We selected a simple random sample of 150 approved requests using the DUA tracking number. We interviewed CMS staff and reviewed SOR notices, CMS policies, and documents in the user agreement files, i.e., the DUA and/or DUA-related documents. We project our findings to our population.

WHAT WE FOUND

For at least 98 percent of all approved data requests in our sample, CMS's disclosures of records were consistent with the routine uses identified in the SOR notices. Five percent of all data files disclosed by CMS were not requested in the DUAs or updated DUAs. CMS did not have the DUAs on file for 33 percent of all user agreement files. The absence of a DUA may limit CMS's ability to verify what data were requested. For 29 percent of the user agreement files, CMS extended entities' use of data without documentation of requests for extensions. Fifteen percent of DUAs were both expired and not closed properly by the entities.

WHAT WE RECOMMEND

We recommend that CMS (1) develop a process to ensure that the data requested are the ones disclosed to the entity; (2) ensure that the DUA and DUA-related documents are in a user agreement file; (3) ensure that entities submit the required documents to properly close their DUAs; (4) use a standardized, documented process for requesting and approving DUA extensions; and (5) ensure that expiration dates are consistent between the DUA and DADSS. CMS concurred with all five recommendations. In its agency response, CMS stated that it was replacing DADSS with the Enterprise Privacy Policy Engine, an electronic information system designed to provide a 100-percent-traceable record of CMS's data disclosures.

TABLE OF CONTENTS

OBJECTIVES

1. To determine whether the Centers for Medicare & Medicaid Services' (CMS) disclosure of individuals' records is consistent with systems of records (SOR) notices required by the Privacy Act.
2. To assess CMS's accounting of individuals' records disclosed to entities between 2006 and 2011.

BACKGROUND

CMS maintains millions of records containing financial and health-related information. Consistent with Federal laws, CMS may disclose the records to entities for certain uses without an individual's prior consent. A record is any item, collection, or grouping of information about an individual maintained by an agency.[1] This information includes, but is not limited to, financial transactions and medical history that contains a name or other unique identifiers.[2] Appropriate safeguards are needed to ensure that the records are disclosed appropriately and that CMS accurately accounts for those disclosures. Inappropriate disclosures can result in loss of privacy and fraudulent activities, such as medical identity theft and inappropriate billing.

The Privacy Act of 1974

The Privacy Act of 1974 (Privacy Act) governs the collection, use, and dissemination of individuals' records maintained in any SOR by Federal agencies, such as those within the Department of Health and Human Services (HHS).[3] An SOR is a group of records under the control of an agency from which information is retrieved using an individual's name or other unique identifier.[4] The Privacy Act prohibits Federal agencies from disclosing a record from an SOR without the individual's written request or prior consent.[5] However, a record may be disclosed without a written request or prior consent for, among other things, the following:

- to agency officers and employees who have a need for the record in the performance of their duties,

[1] 5 U.S.C. § 552a(a)(4), 45 CFR § 5b.1(h).

[2] Ibid. Other unique identifying information can include personally identifiable information, such as a number, symbol, or other identifiers assigned to an individual.

[3] 5 U.S.C. § 552a.

[4] 5 U.S.C. § 552a(a)(5). HHS's regulation implementing the Privacy Act excludes, among other things, records not retrieved by personal identifiers and papers maintained and discarded at the discretion of individual HHS employees. 45 CFR § 5b.1(n).

[5] 5 U.S.C. § 552a(b).

- for a routine use that is compatible with the purpose for which the data were collected,
- for statistical or research purposes,[6] and
- to another agency or government entity for civil or criminal law enforcement activity pursuant to a written request.[7]

CMS SORs

CMS maintains SORs in accordance with the Privacy Act. CMS's SORs contain the records of millions of individuals, such as providers and beneficiaries enrolled in Medicare, Medicaid, and the Children's Health Insurance Program. Examples of SORs maintained by CMS include the National Claims History (NCH) file;[8] Enrollment Database (EDB);[9] Medicare Provider Analysis and Review (MEDPAR) file;[10] and the Provider Enrollment, Chain, and Ownership System (PECOS) database.[11]

The Privacy Act requires that CMS provide public notice in the Federal Register about the existence of each SOR.[12] Each SOR notice is to include, among other things, a description of the individuals for whom the records are collected and maintained and policies and practices regarding storage, retrieval, retention, and disposal of the records and controls for accessing them. Additionally, the SOR notice defines the appropriate routine use and disclosure of the records, which includes the purposes for which CMS collects and maintains records and the types of entities and purposes for which CMS may disclose a record without an individual's prior consent.[13]

---

[6] This requires adequate written assurances that the records will be used solely for statistical or research purposes and that the records will be transferred in a form that is not personally identifiable.

[7] 5 U.S.C. § 552a(b).

[8] The NCH file maintains billing and utilization data on Medicare beneficiaries enrolled in Parts A and B. 71 Fed. Reg. 67137 (November 20, 2006).

[9] EDB maintains information on Medicare enrollment and is used primarily to administer the Medicare program. 73 Fed. Reg. 10249 (February 26, 2008).

[10] MEDPAR maintains Medicare beneficiary information on all services rendered during a stay at an inpatient hospital and/or a skilled nursing facility. 71 Fed. Reg. 17470 (April 6, 2006).

[11] PECOS maintains information on Medicare provider and supplier enrollment, payment, and business history that may include reported exclusions, sanctions, or felonious behavior. 71 Fed. Reg. 60536 (October 13, 2006).

[12] 5 U.S.C. § 552a(e)(4).

[13] 5 U.S.C. § 552a(b)(3). In general, disclosures of Privacy Act-protected records may not be made without an individual's prior consent. However, there are 12 exceptions, including 1 for routine uses identified in the SOR notice. 5 U.S.C. § 552a(b).

CMS Disclosure of Records for Routine Use

CMS's disclosure of records without prior consent must be consistent with circumstances specified in the Privacy Act (e.g., disclosures consistent with the routine uses identified in the SOR notices, disclosures for law enforcement activity, or disclosures for statistical or research purposes) and other applicable rules.[14] CMS's published routine uses include, but are not limited to, maintaining, updating, and disseminating beneficiary[15] and provider[16] information, such as that used for research purposes; supporting program-integrity-related activities of Medicare, Medicaid, or the Children's Health Insurance Program;[17] and ensuring proper Medicare or Medicaid enrollment and payments.[18]

CMS may disclose records to various types of entities for routine uses. Examples of such entities are government agencies, which include HHS employees[19] and law enforcement; disproportionate share hospitals (DSH);[20] and individual or private sector researchers.[21] CMS policy requires that entities complete and submit documentation to CMS prior to disclosing any records. Examples of such documentation include an applicable data use agreement (DUA) and DUA-related documents.[22]

DUA. In most cases, CMS requires that entities requesting records from an SOR (data) submit a DUA and other required documentation.[23] A DUA is the legally binding agreement[24] that CMS uses to ensure its disclosures are in compliance with the Privacy Act requirements. The

---

[14] Other applicable rules may include the HHS Privacy Act regulations, 45 CFR pt. 5b; the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, 45 CFR pt. 164, subparts A and E; and Office of Management and Budget rules governing the safeguarding of personally identifiable information.

[15] 73 Fed. Reg. 2257 (January 14, 2008).

[16] 63 Fed. Reg. 40297 (July 28, 1998).

[17] 71 Fed. Reg. 77759 (December 27, 2006).

[18] 73 Fed. Reg. 10249 (February 26, 2008); 73 Fed. Reg. 11638 (March 4, 2008).

[19] HHS employees include those officers and employees who have a need for the record in performing their duties. 5 U.S.C. § 552a(b)(1).

[20] A DSH is a hospital with a disproportionately large share of low-income patients. CMS, *Medicare Disproportionate Share Hospital*, ICN 006741. January 2013. A DSH may request its cost-reporting data to calculate its Medicare DSH reimbursement amount.

[21] 5 U.S.C. § 552a(b).

[22] CMS, *Policy for Privacy Act Implementation and Breach Notification*, Document Number CMS-CIO-POL-PRIV01-01, p. 6. July 23, 2007.

[23] CMS, op. cit., p. 6. CMS requires contractors and external entities to enter into a DUA for the purpose of tracking disclosures. CMS does not require operational contractors, such as Medicare Administrative contractors, or third parties that have contracts with operational contractors to enter into a DUA because their contracts include language covering compliance with other Federal privacy requirements. Operational contractors are those that perform the work of CMS by paying claims or processing enrollments.

[24] Ibid., p. 21.

DUA contains the written terms and conditions that govern each disclosure.[25] CMS requires that the entity sign the DUA when requesting data. Among other things, the DUA specifies the name of the person who is requesting and responsible for the data; the data requested; the purpose for which the data will be used; and the length of time the data will be retained, known as the retention date.[26] The DUA is the only document by which CMS can verify what data an entity requested. The DUA is necessary to ensure compliance with the accounting requirements under the Privacy Act and the additional safeguards in CMS's policy. Each DUA may include a data request from more than one SOR. For example, an entity may request data from the NCH and the EDB SORs in a single DUA.

CMS has different DUAs for entities requesting data. The type of entity and the type of data—data with specific direct identifiers or limited data—determine which DUA an entity submits to CMS. Data with specific direct identifiers contain beneficiary-specific or physician-specific information. Limited data do not contain specific direct identifiers. All these different DUAs specify what information CMS requires before disclosing any data. These DUAs are:

- A standard DUA, which is the default DUA that entities use to request data with specific direct identifiers, such as data from the NCH or EDB SORs.
- A DSH DUA, which is used only by a DSH that is specifically requesting its cost-reporting data.
- A DUA for a limited data set, which is used by entities requesting data that exclude specific direct identifiers, such as certain data from the MEDPAR SOR.
- A customized DUA, which may be used by a specific type of government agency or government agency contractor, such as an oversight or law enforcement agency.[27]

DUA-related documents. CMS often requires that entities requesting data also submit other applicable DUA-related documents. These documents could include, among other things, an updated DUA, a DUA addendum, a

[25] CMS, *Data Use Agreement: Agreement for Use of Centers for Medicare & Medicaid Services Data Containing Individual Identifiers*, Form CMS-R-0235. Accessed at http://www.cms.gov/cmsforms/downloads/cms-r-0235.pdf. on Aug. 8, 2011.
[26] CMS, *Policy for Privacy Act Implementation and Breach Notification*, Document Number CMS-CIO-POL-PRIV01-01, p. 6. July 23, 2007; Ibid.
[27] Examples of oversight or law enforcement agencies are HHS OIG and the Department of Justice (DOJ).

research study protocol,[28] and institutional review board (IRB) documentation.[29] An updated DUA is used by an entity with an existing DUA to request additional data. A DUA addendum is used if anyone other than the requestor or custodian of the record will handle the requested CMS data or if the original requestor and/or custodian are to be replaced on the DUA.

CMS's Data Request Review and Approval Process

CMS uses a data request review and approval process to ensure that data are disclosed appropriately. The data request review and approval process is initiated when an entity submits a DUA and DUA-related documents to CMS. If CMS approves the data request, it signs the DUA acknowledging the appropriateness of the entity's data request. According to CMS policies and procedures, the data request review and approval process varies by the type of data requested by an entity and the type of entity requesting the data. If CMS approves the data request, it also signs the DUA.

Researchers. CMS requires researchers to submit their DUA and other required DUA-related documents to the Research Data Assistance Center (contractor).[30] The contractor ensures that researchers submit all the required documents prior to the disclosure of data. These required documents include, but are not limited to, the DUA; IRB approval, when necessary; proof of research funding; grant award letters; and research study protocols. Depending on the kind of data they are requesting from CMS, researchers may submit a standard DUA or a DUA for limited data sets. The contractor reviews the documents for appropriateness and completeness and forwards all the documents to CMS for review and approval.

DSHs. DSHs requesting their cost-reporting data submit only DSH DUAs when requesting data. DSHs request cost-reporting data maintained in MEDPAR to calculate their Medicare DSH reimbursement amounts. DSHs specify in the DSH DUAs the years for which they are requesting MEDPAR data. CMS reviews the request and decides whether to approve the DUA.

Government agencies. CMS requires that government agencies and government agency contractors submit only their DUAs when requesting

---

[28] A research study protocol outlines how a study will be conducted.

[29] IRB documentation includes documentation that an IRB or a privacy board has approved a waiver of participant's authorization of use or disclosure of information. Research Data Assistance Center, *IRB Evidence of Approval.* Accessed at http://www.resdac.org/cms-data/request/materials/irb-evidence-approval on September 18, 2012.

[30] CMS contracts with the Research Data Assistance Center to review DUAs from researchers.

data. Examples of such entities are HHS, CMS, CMS contractors, DOJ, HHS OIG, the Social Security Administration, and State Medicaid agencies. Government agencies and government agency contractors requesting data from CMS, such as data from NCH and PECOS, may use a standard DUA or a DUA for a limited data set. In some case, a specific type of government entity or government agency contractor—such as an oversight or law enforcement agency, which has independent authority to obtain the requested data—may use a customized DUA. The customized DUA must indicate what information is being requested and for what purpose the data are being requested. CMS policy does not exempt oversight or law enforcement agencies from using a DUA.

CMS Accounting of Disclosed Records

The Privacy Act requires a Federal agency, such as CMS, to implement safeguards that protect records maintained in an SOR and to account for any disclosures.[31] CMS is required to keep an accurate accounting of the date, nature, and purpose of each disclosure.[32] The accounting should also include the name and address of the entity that received the data.[33] CMS must retain its accounting of the disclosure for at least 5 years after the disclosure or for the life of the data, whichever is longer.[34]

CMS promulgated its *Policy for Privacy Act Implementation and Breach Notification* to implement the requirements of the Privacy Act.[35] CMS policy states that disclosures "shall be limited to that which is necessary to accomplish the intended purpose of an Agency activity" and that "CMS shall limit the disclosures of personally identifiable information to no greater amount of information than is reasonably necessary to achieve the specific purpose of the disclosure."[36] In addition, CMS policy states, "A

---

[31] 5 U.S.C. § 552a(c).

[32] 5 U.S.C. § 552a(c)(1)(A).

[33] 5 U.S.C. § 552a(c)(1)(B).

[34] 5 U.S.C. § 552a(c)(2); Pursuant to CMS's *Records Schedule*, Section I: Administrative/Management Records, S: Data Use Agreements, 1b: Master Data Files. November 2012. Accessed at http://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/downloads/RecordsSchedule.pdf on April 24, 2013. CMS notes that under General Records Schedules (GRS) 24.6(a) of the National Archives and Records Administration (NARA), accounting of disclosures should be retained for 6 years after the DUA is terminated or no longer needed for investigative or security purposes, whichever is later. NARA GRS, GRS 24.6(a). April 2010. Accessed at http://www.archives.gov/records-mgmt/grs/grs24.html on May 7, 2013.

[35] CMS, *Policy for Privacy Act Implementation and Breach Notification*, Document Number CMS-CIO-POL-PRIV01-01, p. 1. July 23, 2007.

[36] Ibid., p. 3.

record of disclosures shall be maintained for all required Privacy Act disclosure."[37]

Data Agreement and Data Shipping Tracking System (DADSS). CMS uses DADSS as an automated database to track and account for approved data requests, DUAs, and disclosures under the Privacy Act and its policies. DADSS generates a DUA tracking number for each approved data request, which CMS uses to track the data disclosed to an entity. DADSS contains some, but not all, of the same information as the DUA, updated DUA, and DUA addenda.

For approved data requests, CMS enters information from the DUA, the updated DUA, and the DUA addendum into DADSS. CMS also enters additional information in DADSS, such as the type of entity requesting the data; routine use for which the data is being disclosed; DUA extension date and number of extensions, if applicable; and data disclosed to the entity. CMS, however, does not keep electronic copies of the DUA, updated DUA, or DUA addendum in DADSS. Hard copies of the DUA and DUA-related documents are kept in a user agreement file.

CMS uses DADSS to send automated emails reminding entities about upcoming DUA expiration dates. The emails are sent 90, 60, and 30 days prior to the expiration date.

DUA closure or extension. CMS policy requires that entities properly close their DUAs or request to extend them on or before the expiration dates specified in the DUAs.[38] Entities may close their DUAs prior to the expiration dates when they no longer need the data. During the period of our review (July through November 2011), CMS required that to properly close a DUA, entities return the data[39] or complete a certificate of data destruction form (referred to as data destruction form).[40] By completing and submitting the data destruction form, entities certified that they destroyed all data, and any copy of the data, listed in the DUA.

CMS required that to request extensions entities submit written requests—typically via email—explaining why extensions were needed.[41] CMS

---

[37] Ibid., p. 4.

[38] Ibid., p. 6.

[39] Returned data are to be accompanied with a cover letter indicating the study or project name and the name of the data being returned.

[40] CMS, Form CMS-R-0235, p. 3; see also *Certificate of Data Destruction for Data Acquired from CMS*, Form CMS-10252.

[41] CMS, *DUA – Extensions and Closures*. Accessed at http://www.cms.gov/PrivProtectedData/27_DUA-Extensions_Closures.asp on June 22, 2011.

indicated that it would not approve new data requests from entities with expired DUAs.

Related Work

This evaluation is part of a body of Office of Inspector General (OIG) work on privacy and the protection of personally identifiable information. OIG has conducted work related to medical identity theft[42] and the HIPAA Security Rule.[43] In addition, OIG is concurrently conducting work on the HIPAA Privacy Rule[44] and the Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification Rule.[45]

In 2012, the Government Accountability Office (GAO) provided Congressional testimony on the Federal Government's use and collection of personally identifiable information.[46] GAO recommended that Congress consider amending applicable privacy laws to address vulnerabilities arising from increased dependence on information technology. Such vulnerabilities can result in compromising sensitive personal information.

METHODOLOGY

Scope

We reviewed data requests approved or renewed by CMS between September 2006 and August 2011. We selected this 5-year timeframe to account for DUAs that were active for more than 1 year. We reviewed only approved data requests entered in DADSS.

We limited our review to approved data requests from health-related SORs. Examples of health-related SORs include those that maintain beneficiary or provider claims information. We did not include approved data requests from non-health-related SORs, such as those that maintain information on employee access to CMS facilities and individuals ordering provider educational materials.

---

[42] OIG, *Breaches and Medical Identity Theft Involving Medicare Identification Numbers*, OEI-02-10-00040, October 2012.

[43] OIG, *Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight*, A-04-08-05069, May 2011.

[44] OIG, *Office for Civil Rights (OCR) Oversight of the HIPAA Privacy Rule,* OEI-09-10-00510.

[45] OIG, *OCR Oversight of Covered Entities' Compliance with the HITECH Breach Notification Rule*, OEI-09-10-00511.

[46] GAO, *Federal Law Should Be Updated to Address Changing Technology Landscape*, GAO-12-96IT. Accessed at http://www.gao.gov/assets/600/593146.pdf on October 9, 2012.

Sample Selection

We used the DUA tracking number generated by DADSS to identify our population of approved data requests. Our population consisted of 5,108 approved data requests. We selected a simple random sample of 150 approved data requests from this population using the DUA tracking number. Our sample contains 396 data file requests. These data files come from 19 SORs. We project our findings to our population of approved data requests. See Appendix A for a table listing the confidence intervals.

Data Collection and Analysis

We used the following data sources for our evaluation: (1) CMS policies and procedures, (2) CMS staff interviews, (3) SOR notices, and (4) user agreement files, i.e., DUA and/or DUA-related documents.

CMS policies and procedures. We reviewed CMS's policies and procedures to understand CMS's process for approving data requests, DUA extensions, and DUA closures. We also reviewed CMS's policies and procedures for the disclosure and accounting of data.

CMS staff interview. We conducted a structured interview with CMS staff responsible for approving data requests and the disclosure and accounting of data. We asked CMS staff how they approved data requests, granted DUA extensions, closed DUAs, and accounted for the disclosures.

SOR notices. We reviewed each of the SOR notices associated with our sample to identify the routine uses allowed for the disclosure of the data.

User agreement files. We requested paper or scanned versions of the DUAs and any DUA-related documents associated with each approved data request in the sample. For the purposes of this report, we refer to each set of DUA and/or its corresponding DUA-related documents as a user agreement file. The number of user agreement files corresponds with the number of approved data requests in our sample. A DUA and/or its DUA-related documents, such as the updated DUA, DUA addenda, DADSS documentation, requests for extensions, and data destruction forms, constitute a user agreement file.

User Agreement Files Analysis

We analyzed the user agreement files on three levels—the user agreement file level, DUA level, and data file level.

User agreement file level. We reviewed the documents in the user agreement files to determine the purpose for which the data were requested. We reviewed the routine use category on the DADSS documentation to identify the purpose of the data request. We calculated the percentage of approved data requests that were requested under CMS's

routine use categories. Also, we reviewed DADSS documentation in the user agreement files to determine what types of data CMS disclosed to entities. We identified and calculated the percentages of the types of data requested using the SORs listed in the DADSS documentation.

We reviewed the documents in the user agreement files to determine whether the approved data requests, as documented in DADSS, had a DUA on file. We calculated the percentage of user agreement files that did not include the DUA. Of these user agreement files that were missing a DUA, we calculated the percentage that had DADSS and DUA-related documents and the percentage that had only DADSS documentation. We also calculated the percentage of user agreement files that did not have a DUA, DADSS documentation, and any other DUA-related documents.

We reviewed the user agreement file to identify documentation of requests for extensions from an entity. We calculated the percentage of user agreement files that did not include any documentation of the entity requesting to extend their DUA.

DUA level. We reviewed the expiration dates of the DUAs associated with our sample of approved data requests. We identified the expiration dates for each DUA and noted inconsistencies, if any, between the expiration date listed on the DUA and that in the DADSS documentation. We calculated the percentage of DUAs that were expired and not closed properly as of November 17, 2011. This is the date for which we collected the user agreement files from CMS. In addition, we calculated how long the DUAs have been expired.

We identified DUAs that had inconsistent expiration dates between the DUA and DADSS documentation. We calculated the percentage of DUAs for which the DUA and the DADSS documentation had inconsistent expiration dates.

Data file level. To determine whether CMS disclosed the appropriate data file requested by the entities, we compared the data file on the DUAs or updated DUAs with the data file listed on the DADSS documentation. We used the DUAs and updated DUAs to identify the data file requested by the entity. We used the DADSS documentation to identify the data file disclosed to the entity. We calculated the percentage of data files that did not match the data file requests on the DUAs or updated DUAs.

Limitations

Our analysis was limited to the information provided by CMS and the information on the DUAs, DUA-related documents, and DADSS. We did not contact the entities that were in our sample of approved data requests to verify what data were disclosed to them. Further, we did not contact the

entities to determine whether each needed to submit a data destruction form prior to its DUA's expiration date because it no longer needed the data. We did not determine whether the data disclosures violated the Privacy Act.

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

For at least 98 percent of all approved data requests, CMS's data disclosures were consistent with the routine uses

For 98 percent of all approved data requests in our sample, DADSS documentation indicated that CMS's data disclosures were consistent with the routine uses identified in the SOR notices. Of the 98 percent, 46 percent were for the routine use of Medicare cost-reporting data requested by hospitals that may be entitled to DSH payments.[47] Additionally, 33 percent of approved data requests were for research purposes, 18 percent were for routine use by Federal agencies, and 4 percent were for routine use by State agencies.[48]

For the remaining 2 percent of all approved data requests in our sample, it is unknown whether the disclosures were consistent with the routine uses. None of these approved data requests had the DUAs on file. In two instances, DADSS documentation was also not available. Without the DUA and DADSS documentation, it would be difficult for CMS to identify what the purpose of the request was or what data were requested or disclosed. In another instance, the data disclosure was listed as "Other data (specify)" in the DADSS documentation. However, there was no indication of the specific data released to the entity. Thus, CMS would not know what data were disclosed.

CMS disclosed data files not requested in the DUAs or updated DUAs

Five percent of all data files disclosed by CMS were not requested in the DUAs or updated DUAs associated with our sample of approved data requests.[49] The data were disclosed to Federal agencies and researchers. Some of the disclosed data were outside the date ranges indicated on the DUAs or updated DUAs. In other instances, an entity requested a specific NCH file in the DUA but DADSS documentation indicated that a different NCH file was disclosed. Most of the data disclosed were from the NCH and EDB SORs. The remaining data came from various SORs that included Medicare provider, beneficiary, drug, and payment data.

[47] This percentage combines all routine use categories used by CMS for DSHs and CMS components requesting Medicare cost-reporting data on behalf of DSHs.

[48] Because of rounding, these percentages do not add up to 100 percent.

[49] The DUA or updated DUA may include a request for a data file from more than one SOR.

One-third of all user agreement files did not include the DUAs

CMS policy requires a DUA for data disclosures; however, CMS did not have the DUAs on file for 33 percent of all user agreement files associated with our sample of approved data requests.[50] Among the 33 percent, 18 percent had DADSS documentation and other DUA-related documents. Seventy-eight percent of user agreement files that did not have the DUAs had only DADSS documentation. No other documents, such as the updated DUA, DUA addenda, and other DUA-related documents, were included in those user agreement files. For the remaining 4 percent, CMS had approved the requests and assigned DUA tracking numbers but could not account for the DUAs, DUA-related documents, or DADSS documentation in the user agreement files. According to CMS staff, the DUAs or DUA-related documents may have been misfiled or misplaced. See Table 1 for the percentage of user agreement files without the DUAs, DUA-related documents, or DADSS documentation.

Table 1: User Agreement Files Without the DUAs

User agreement file documents	Percentage of user agreement files
No DUA but DADSS documentation and DUA-related documents were in the user agreement file	18%
No DUA and only DADSS documentation were in the user agreement file	78%
No DUA, no DUA-related documents, and no DADSS documentation were in the user agreement file[51]	4%

Source: OIG analysis of user agreement files, 2012.

Although, CMS can use DADSS to identify whom the data were disclosed to, what type of data was disclosed, and for what purpose CMS disclosed the data, DADSS would not have the signed DUA, which includes the agreed upon terms and conditions that govern the disclosure. In addition, the absence of a DUA may limit CMS's ability to verify what data were requested, for what purpose the data were requested, how long the data may be retained, and who is responsible for and may use the data. Specifically, if CMS entered inaccurate or incomplete information from the DUA into DADSS, CMS would be limited to relying on the information available in DADSS or would need to follow up with the

[50] DADSS generates a DUA tracking number for each approved data request, which CMS uses to track the data disclosed to an entity.

[51] Although DUA tracking numbers for these approved data requests were entered in DADSS at the time of our sample selection, CMS did not provide OIG with any associated documentation from the user agreement files, such as DADSS documentation, for review.

entity to verify information that may have been included in the DUA or DUA-related documents.

CMS granted DUA extensions without documentation of requests from the entities

For 29 percent of the user agreement files associated with our sample of approved data requests, CMS lacked documentation of a request for a DUA extension. Although CMS did not have any documentation, it granted DUA extensions to entities. The entities for which CMS granted the extensions included researchers and government agencies. The amount of time for which the extensions were granted is unknown because no previous expiration dates were noted in the DADSS documentation or the DUAs were not on file. Additionally, some of these entities had already requested extensions prior to receiving additional extensions from CMS.

Fifteen percent of all DUAs were expired and not closed properly

Fifteen percent of all DUAs associated with our sample of approved data requests were both expired and not closed properly by the entities in accordance with CMS policy. None of these entities submitted data destruction forms. Further, there was no documentation in the user agreement file indicating that the entities returned the data. The data requested under these expired DUAs remain with the entities. Of these DUAs, 48 percent have been expired for almost a year and the remaining 52 percent have been expired for a year or more. Three entities that had requested and received extensions still had expired DUAs.

Additionally, 13 percent of all DUAs associated with our sample of approved data requests had DADSS documentation with expiration dates that were not consistent with those on the DUAs. The difference between the expiration dates on the DUAs and in the DADSS documentation ranged from 3 weeks to 3 years. In eight cases, the expiration dates in the DADSS documentation came before the expiration dates on the DUAs.

CONCLUSION AND RECOMMENDATIONS

For at least 98 percent of all approved data requests in our sample, CMS's disclosures of records were consistent with the routine uses identified in the SOR notices. For the remaining 2 percent, it was unknown whether the disclosures were consistent with the routine uses. Five percent of all data files disclosed by CMS were not requested in the DUAs or updated DUAs. CMS policy requires a DUA for data disclosures; however, CMS did not have the DUAs on file in 33 percent of all the user agreement files. For 29 percent of user agreement files, CMS lacked documentation of a request for a DUA extension. Fifteen percent of all DUAs associated with our sample of approved data requests were both expired and not closed properly by the entities in accordance with CMS policy. Further, 13 percent of DUAs associated with our sample of approved data requests had expiration dates inconsistent with those in DADSS.

Overall, CMS's data disclosures are consistent with the routine uses identified in the SOR notices. However, CMS's system of tracking and accounting for disclosures needs improvement. The Privacy Act requires that CMS keep an accurate accounting of the disclosed data. Although CMS may have a record of the approved data request in DADSS, it would not have the signed DUA, which contains the agreed-upon terms and conditions that govern the disclosures. Also, the DUA is necessary to ensure compliance with the accounting requirements under the Privacy Act and the additional safeguards in CMS's policy. CMS is working towards upgrading DADSS with the Enterprise Privacy Policy Engine (EPPE) system, an electronic information system designed to provide a traceable record of CMS's disclosures. Without accurate accounting, vulnerabilities exist in CMS's tracking and accounting of data disclosures.

We recommend that CMS:

Develop a Process To Ensure That the Data Requested Are the Ones Disclosed to the Entity

CMS should develop a process to ensure that the disclosed data are the ones requested by the entity. CMS could integrate an electronic form in DADSS to track and compare what data were requested and what data were disclosed to the entity. When additional data requests are made under the same DUA, CMS could add the request and disclosure on the electronic form to track and account for the data. Further, when using the "Other data (specify)" category, CMS could specify on the electronic form what data were requested and disclosed to the entity.

Ensure That the DUA and DUA-Related Documents Are in a User Agreement File

CMS should ensure that all required DUA and DUA-related documents, such as the updated DUA, requests for extensions, and data destruction forms, are in a user agreement file.

CMS could use DADSS or another system to electronically store or file the DUAs and DUA-related documents. Electronic storage could potentially prevent paper DUAs and DUA-related documents from being misplaced or misfiled. Currently, CMS is working on a paperless user agreement submission process to help with electronic filing.

Ensure That Entities Submit the Required Documents To Properly Close Their DUAs

CMS should ensure that entities submit the required documents to properly close their DUAs. In June 2012, CMS made changes to its DUA closure policy. CMS has replaced the data destruction form with a certificate of disposition form. Entities can use the certificate of disposition form to close DUAs by indicating that they are destroying all the data listed in the DUA or are reusing all or some of the data in other DUAs. Additionally, CMS should not rely solely on the automated expiration date email reminders. CMS should continue to follow up with entities that have expired DUAs.

Use a Standardized, Documented Process for Requesting and Approving DUA Extensions

During the period of our review, CMS relied on emails from entities to request extensions on their DUAs. However, email requests may be lost, deleted, or misfiled, leaving CMS without any proof that the entities requested extensions. Instead of an emailed request, CMS could require that entities request extensions using the certificate of disposition form. CMS could ensure that extension requests are approved only when the entities submit completed certificate of disposition forms. The forms could include information that entities provided in their emailed requests for extension. The use of one form to close or extend a DUA could streamline CMS's process for tracking the status of the approved data requests, DUAs, and disclosed data.

Ensure Consistent Expiration Dates Between the DUA and DADSS

CMS should ensure that the expiration date entered in the DUA is consistent with that in DADSS. If expiration dates are incorrect, CMS may fail to send email reminders about approaching expiration dates or may email entities the wrong dates.

Recent changes by CMS could address some of the problems we identified with the expiration dates. CMS has limited the timeframe for which entities may retain the data. DUAs are set to expire 1 year from the approval date. An entity must revalidate its DUA annually with CMS if the data are needed after the initial expiration date. CMS does not limit the number of times that an entity may request an extension.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS concurred with all five of our recommendations.

CMS concurred with our first recommendation and stated that it is replacing and upgrading DADSS. CMS explained that the replacement system, the EPPE system, is designed to provide a 100-percent-traceable record of CMS's data disclosures. Although the EPPE system is designed to trace the records disclosed, CMS should ensure that the data requested are the ones that are disclosed to the entity.

CMS concurred with our second recommendation and stated that the EPPE system will maintain an automated filing of all DUA-related documents.

CMS concurred with our third recommendation and stated that the EPPE system will provide a central catalog of what data were disclosed and to whom they were disclosed. While the EPPE system is designed to maintain an accounting of all DUA-related actions and establish an automated workflow for approval of access to data, CMS should implement a process to ensure that entities submit the required documents to properly close their DUAs.

CMS concurred with our fourth recommendation and stated that the EPPE system is being designed to standardize the process for an automated accounting of all DUA-related actions. CMS should ensure that the EPPE system will include a process for standardizing the request and approval of DUA extensions.

CMS concurred with our fifth recommendation and stated that it will use the EPPE system to ensure consistent expiration dates between the DUA and DADSS. CMS explained that the EPPE system is being designed to provide consistency in the accounting of all DUA-related actions.

See Appendix B for the full text of CMS's comments.

APPENDIX A

Point Estimates and Confidence Intervals

We calculated the point estimates and confidence intervals for data points from our sample of approved data requests. The sample sizes, point estimates, and 95-percent confidence intervals are provided for the following:

Table A-1: Point Estimates and Confidence Intervals

Estimate Description	Sample Size	Point Estimate	95-Percent Confidence Interval
Percentage of approved data requests for which the Centers for Medicare & Medicaid Services' (CMS) disclosure of data was consistent with the routine uses	150 approved data requests	98.0%	94.3%–99.6%
Percentage of approved data requests for which the routine use was providing the Medicare cost-reporting data requested by hospitals that may be entitled to DSH payments	147 approved data requests that were consistent with routine uses	45.6%	37.4%–53.7%
Percentage of approved data requests for which the routine use was research	147 approved data requests that were consistent with routine uses	32.7%	25.0%–40.3%
Percentage of approved data requests for which the routine use was use by Federal agencies	147 approved data requests that were consistent with routine uses	17.7%	11.9%–24.8%
Percentage of approved data requests for which the routine use was use by State agencies	147 approved data requests that were consistent with routine uses	4.1%	1.5%–8.7%
Percentage of approved data requests for which it is unknown whether CMS's disclosure of data was consistent with the routine uses	150 approved data requests	2.0%	0.4%–5.7%
Percentage of data files disclosed by CMS but not requested in the DUA or updated DUA	396 data files	5.1%	1.5%–8.6%
Percentage of user agreement files that did not include a DUA	150 user agreement files	33.3%	25.7%–41.0%
Of user agreement files that did not include a DUA, percentage of user agreement files that had Data Agreement and Data Agreement and Data Shipping Tracking System (DADSS) documentation and other DUA-related documents	50 user agreement files that did not include a DUA	18.0%	8.6%–31.4%
Of user agreement files that did not include a DUA, percentage of user agreement files that had only DADSS documentation	50 user agreement files that did not include a DUA	78.0%	64.0%–88.5%
Of user agreement files that did not include a DUA, percentage of user agreement files that had neither DADSS documentation nor DUA-related documents	50 user agreement files that did not include a DUA	4.0%	0.5%–13.7%
Percentage of DUAs for which CMS extended the expiration dates without requests for extensions from the entities	150 DUAs	28.7%	21.4%–36.0%
Percentage of DUAs that were both expired and not closed properly	150 DUAs	15.3%	10.0%–22.1%
Of the DUAs that were both expired and not closed properly, percentage of DUAs that were expired for almost a year	23 DUAs that were both expired and not closed properly	47.8%	25.7%–69.9%

Continued on next page

Table A-1: Point Estimates and Confidence Intervals (Continued)

Estimate Description	Sample Size	Point Estimate	95-Percent Confidence Interval
Of the DUAs that were both expired and not closed properly, percentage of DUAs that were expired for a year or more	23 DUAs that were both expired and not closed properly	52.2%	30.1%–74.3%
Percentage of DUAs that had no expiration dates in the DUA or DADSS documentation	150 DUAs	10.7%	6.2%–16.7%
Percentage of DUAs for which the DUA and DADSS documentation had inconsistent expiration dates	150 DUAs	12.7%	7.8%–19.1%

Source: Office of Inspector General analysis of user agreement files, 2012.

APPENDIX B

Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

JUN 18 2013

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner /S/
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report - *CMS' Disclosure and Accounting of Data Under the Privacy Act*, OEI-09-11-00430

Thank you for the opportunity to review and comment on the above mentioned OIG draft report. The Centers for Medicare & Medicaid Services (CMS) appreciates the contributions and valuable input by the OIG. The draft report assessed CMS' disclosure and accounting of data under the Privacy Act. The information in the report will help inform our administration of CMS' implementation of the Privacy Act.

We are continuously working to improve our implementation of the Privacy Act and accountability for personally identifiable information (PII) disclosures from CMS' systems of records (SOR). The draft report contained five recommendations for CMS. We are addressing the recommendations in this response.

OIG Recommendation

CMS develop a process to ensure that the data requested are the ones disclosed to the entity.

CMS Response

We concur with this recommendation. CMS is currently in the process of replacing and upgrading the Data Agreement and Data Shipping Tracking System which CMS uses to track the disclosures of CMS PII. The replacement system, the Enterprise Privacy Policy Engine (EPPE), is designed to provide a 100% traceable record of CMS' PII disclosures.

OIG Recommendation

CMS should ensure that the DUA and DUA-related documents are in a user agreement file.

CMS Response

We concur with this recommendation. CMS' EPPE system is designed to maintain a 100% automated filing of all DUA related documentation.

OIG Recommendation

CMS should ensure that entities submit the required documents to properly close their DUAs.

CMS Response

We concur with this recommendation. The CMS' EPPE system will be designed to maintain a 100 percent accounting of all DUA related actions. It will provide a central catalog of CMS personally identifiable information and the individuals and organizations that were disclosed, thereby providing a complete audit trail of all disclosures of CMS PII. It will establish automated workflows for approval of access to CMS PII data and automate requests for creating, tracking and disseminating PII data media shipments, as well as improve the user experience, interface and management techniques for requesting CMS data.

OIG Recommendation

CMS should use a standardized, documented process for requesting and approving DUA extensions.

CMS Response

We concur with this recommendation. The CMS' EPPE system is being designed to standardize the process for a 100% automated accounting of all DUA related actions.

OIG Recommendation

CMS should ensure consistent expiration dates between the DUA and DADSS.

CMS Response

We concur with this recommendation. The CMS' EPPE system is being designed to provide 100% consistency in the accounting of all DUA related actions.

The CMS appreciates the effort that went into this draft report and we look forward to continuing to work with you in the future.

Attachment

ACKNOWLEDGMENTS

This report was prepared under the direction of Timothy Brady, Regional Inspector General for Evaluation and Inspections in the San Francisco regional office, and Michael Henry, Deputy Regional Inspector General.

Abby Lopez served as the project leader for this study. Other Office of Evaluation and Inspections staff from the San Francisco regional office who conducted the study include Camille Harper. Central office staff who provided support include Clarence Arnold, Kevin Manley, Christine Moritz, and Tasha Trusty.

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.