



Comments of the World Privacy Forum

On

Proposed Centers for Medicare & Medicaid Services rule, Medicare Program; Medicare Part D Data (CMS-4119-P)

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-4119-P
Mail Stop C4-26-05
7500 Security Boulevard
Baltimore, MD 21244-1850

December 14, 2006

VIA overnight mail and electronic submission

Re: Proposed rule, Medicare Program; Medicare Part D Data (CMS-4119-P)

This is a comment on the proposed rule (file code CMS-4119-P) by the Centers for Medicare & Medicaid Services that would allow the Secretary of Health and Human Services to use the claims information that is now being collected for Part D payment purposes for other research, analysis, reporting, and public health functions. The proposal appears in 71 Federal Register 61445 (October 18, 2006).

The World Privacy Forum is a non-profit, non-partisan public interest research organization. It focuses on in-depth research and analysis of privacy topics. See <http://www.worldprivacyforum.org>. Our concerns about the proposed rule relate exclusively to the effect of the proposal on the privacy rights and interests of plan beneficiaries. We offer no comment on the effect of the proposal on the interests of providers, plans, or sponsors.

I. Background

The background section for the proposed rule explains that the purpose of the rule is to resolve what CMS calls the “statutory ambiguity” involving the limit found in Section 1860D-15 of the Social Security Act (42 U.S.C. § 1395w-115). The key provision of the Act states:

(f) DISCLOSURE OF INFORMATION.—

(2) RESTRICTION ON USE OF INFORMATION.—Information disclosed or obtained pursuant to the provisions of this section may be used by officers, employees, and contractors of the Department of Health and Human Services only for the purposes of, and to the extent necessary in, carrying out this section.

Congress expressly placed a restriction on the use of Part D information. What the proposed rule attempts to do, and in a very unconvincing way, is to read these words out of the Act entirely. The effect of the proposed rule is to ignore the limitation on data use and disclosure that Congress placed in the legislation. Instead, CMS is attempting to find a justification for avoiding the restriction because CMS considers that its priorities outweigh the congressional direction. Indeed, CMS proposes a rule that will allow the disclosure of information to hundreds of institutions and tens of thousands of individuals notwithstanding the contrary congressional direction.

The weakness of the CMS argument is underscored by the reference (on page 61447) to a press release issued by the House Ways and Means Committee on the day that the legislation was signed into law by the President. The reference is a weak one, because a committee press release issued long after the legislation finally cleared the Congress has no weight as legislative history. Even if the release were entitled to any weight, the vague statement quoted in the proposed rule does not support the interpretation that CMS places on it. Nothing in the quoted words suggests in any way that the privacy interests of Part D recipients should be ignored.

The proposed rule violates basic principles of statutory construction that require that all words in a statute be given meaning and effect. If there is a conflict or inconsistency between different sections of a law, an agency is obliged to make a greater effort to try to reconcile and not ignore those sections. CMS has made no attempt to do so. It has not explained how it might accomplish other functions in whole or in part by proposing a way to use Part D information without personal identifiers, with partially de-identified information, with encrypted information, or through the use of other privacy protective techniques that allow some use of information while masking the identities of data subjects. Any of these techniques would allow other functions to be completed in some manner while acknowledging the clear congressional purpose of limiting the spread of *identifiable* information.

The proposed rule is entitled to no interpretative deference because of CMS' failure to give any meaning to the words of the law or to explain alternatives. Until CMS goes through the steps of explaining all alternatives to ignoring the congressional direction, it has not sustained its burden of justifying the outcome that it seeks. If CMS cannot reconcile the different sections of the law, we recommend that it return to the Congress and seek clarification of the law.

II. Information to be Collected

The underlying argument in the proposed rule is that CMS could, if it chose to, collect the same information under other provisions of the Act that do not include the restriction on data use. The next step in CMS's argument is that requiring sponsors to submit claims information twice would be duplicative. Therefore, CMS can collect the information once and ignore the restriction

on use. This reasoning is faulty because it does not give any weight to the restrictive language. While we do not propose duplicative submission as a practical alternative, we do not believe that even duplicative submission would justify the proposed rule. CMS cannot do indirectly precisely what the statute prohibits CMS from doing directly.

We repeat that CMS has not justified the proposed rule by considering alternatives that would give at least some weight to the express congressional restrictions on use of Part D information. CMS has not considered the possibility of carrying out other functions in whole or in part using Part D information without personal identifiers, with partially de-identified information, with encrypted information, or through the use of other privacy protective techniques that allow use of information while masking the identities of data subjects.

III. Purpose of CMS Collecting Information

The discussion in the proposed rule explaining what CMS wants to do with the information is fatally flawed because no consideration is given to alternatives that would reflect rather than ignore the data use restrictions in the law. All of the activities that CMS wants to carry out can be accomplished in some fashion while complying with the data use restriction. While obeying the restrictions might not allow for full implementation of all desired activities, CMS could still fulfill some or most of its objectives by using Part D information without personal identifiers, with partially de-identified information, with encrypted information, or through the use of other privacy protective techniques that allow use of information while masking the identities of data subjects.

The thinness of the argument here is underscored by the argument that CMS needs to ignore data restrictions in law in order to make legislative proposals to Congress. Agencies throughout the federal government operate daily under a wide variety of statutory data restrictions, yet they seem fully able to propose new legislation notwithstanding those restrictions. CMS' argument about legislative proposals hints at desperation.

In this section on page 61448, CMS requests "comments on whether there should be any limitations on data when shared for purposes other than fulfilling CMS's responsibility to administer the Part D program." We find this request particularly troubling. Does CMS also propose to ignore the data disclosure limitation in the Privacy Act of 1974 that prevents the use of data collected for one purpose from being used for an incompatible purpose? Will CMS ignore restrictions in the substance abuse rules (42 CFR Part 2) too? How far does CMS want to go in sharing Part D data for other purposes? The proposed rule suggests that CMS can ignore legal restrictions that it finds inconvenient. We disagree, and we think that CMS's failure to acknowledge other legal restrictions in the proposed rule and to indicate how it plans to comply with these other restrictions is a major flaw.

The proposed rule begins by seeking to ignore a statutory restriction on data use in order to fulfill statutory purposes related to Part D. While we do not agree with the proposed CMS rule or justification, we acknowledge that reconciling different parts of the law presents a challenge. However, the suggestion that, notwithstanding the express restrictions, CMS nevertheless has the authority to share the data for wholly unrelated activities only serves to undermine the bona fides

of the proposed rule. Does CMS plan to turn patient records over to law enforcement to begin investigations of wholly unrelated crimes? Will CMS turn over prescription information to pharmaceutical manufacturers who want to market their products to patients? Does CMS recognize any limitation on its authority to share patient information? The breadth of the request for comments is even more troubling than the rest of the proposed rule.

IV. Sharing Data with Entities Outside of CMS

In this section – (Proposed Sec. 423.505(f)(5)) -- the proposed rule states (page 61452):

Given these necessities, we propose to allow broad access for other agencies to our Part D claims data linked to our other claims data files. Other agencies, including the agencies listed above, would enter into a data use agreement, similar to what is used today (and described in greater detail in section II.C.2). This would allow the sharing of event level cost data, however, through a data use agreement we would protect confidentiality of beneficiary information and ensure that the use of Part D claims data serves a legitimate research purpose. We would also ensure that any system of records with respect to claims data is updated to reflect the most current uses of such data. We request comments on this proposed rule that would help us in our efforts to improve knowledge relevant to the public health.

Specifically, we request guidance on how we can best serve the needs of other agencies through the sharing of information it collects under section 1860D–12(b)(3)(D) of the Act while at the same addressing the legitimate concerns of the public and of Part D plans that we appropriately guard against the potential misuse of data in ways that would undermine protections put in place to ensure confidentiality of beneficiary information, and the nondisclosure of proprietary data submitted by Part D plans.

1. We object to the use of the word *necessities* in the first quoted paragraph. Whether or not it would be desirable to undertake the activities discussed in the proposed rule, the statement that these activities are *necessities* goes far beyond anything demonstrated in the predicate to the paragraph. Activities that seek to use data restricted by law are not necessary. Activities that CMS would like to conduct are not necessary.

CMS continues to ignore the statute, first by claiming authority to use data subject to restriction, and now by claiming authority to share data widely throughout the federal government and beyond. Anything that CMS finds convenient or desirable now seems to be a *necessity*. If there is any limitation on the ability of CMS to share confidential patient information with anyone – and we believe that there are several statutory limitations – it is not reflected in this proposed rule.

We once again ask CMS to give effect to the data restrictions that Congress has expressly included in the law.

2. It is impossible to assess the intent of CMS without having the ability to review the system of record notice for the data collected under Part D. Only the system of record notice will explain in

sufficient detail just how far CMS intends to go in sharing patient data. We will not know, for example, if CMS plans to share data with pharmaceutical manufacturers for marketing activities without seeing the routine uses for the system of records.

Publishing this proposed rule without the accompanying system of records notice is a fatal flaw. CMS has only disclosed some of its plans. However, CMS has not told the public how it will accommodate the data use and disclosure restrictions imposed by the Privacy Act of 1974. That information is essential to evaluating the proposed rule. The failure to publish a system of records notice along with the proposed rule makes it impossible for a commenter to fairly assess the full scope and legality proposed rule. A system of records notice is an integral part of any personal data use activity contemplated by a federal agency. We recommend that CMS republish the proposed rule along with all relevant system of records notices that will cover the data in question.

3. In response to the request for guidance for data sharing, we suggest that if any data sharing can be lawfully done under the Part D data restrictions, CMS should allow data sharing of Part D information without personal identifiers, with partially de-identified information, with encrypted information, or through the use of other privacy protective techniques that allow use of information while masking the identities of data subjects. The many techniques for masking the identifiability of data that have been developed by statisticians should be mandated for Part D data if the data is to be shared at all. Aggressive use of identifier protection methods will allow most of the objectives of sharing to be accomplished.

4. Along these lines, we take note of the statement that "[t]his would allow the sharing of event level cost data, however, through a data use agreement we would protect confidentiality of beneficiary information." This statement suggests a fundamental misunderstanding of privacy. Sharing of data is a breach of confidentiality. It exposes the data to new eyes, to additional security breaches, and to new threats to privacy. Undertaking data sharing through a data use agreement can mitigate the threat to privacy, but it does not eliminate it.

We support the use of data use agreements when data must be shared and when it is lawful to share data. However, CMS should realize that the sharing of data – even with the admonition that the data should not be further disclosed – still directly undermines the privacy of data subjects. We acknowledge that data sharing is sometimes justifiable, but that does not mean that privacy interests are unaffected by the sharing. CMS's case for data sharing would be enhanced if it could manage to demonstrate a greater understanding of and sensitivity to privacy.

The proposed rule provides:

See our Agreement for Use of Centers for Medicare and Medicaid Services Data Containing Individual Specific Information at <http://www.resdac.umn.edu/docs/CMS-R-02352-v2-locked.doc>. In addition, we would ensure that our system of records for claims data would permit these usages of the data. We request comments on the proposed use of the data for research purposes that would help CMS in its efforts to improve knowledge relevant to public health. We also ask for comments on whether we should

consider additional regulatory limitations for external researchers beyond our existing data use agreement protocols in order to further guard against the potential misuse of data for non-research purposes, commercial purposes, or to ensure that proprietary plan data or confidential beneficiary data is not released.

1. We were surprised to find that the standard agreement for use of CMS data does not include a requirement that the recipient obtain a certification of confidentiality for all identifiable CMS data covered by the agreement or other data within the scope of the research project. In general, certificates of confidentiality authorize researchers to resist compulsory legal demands (e.g., subpoenas and court orders) for identifiable research information about individuals. By providing a defense against compelled disclosure, certificates provide a defense against legal obligations to disclose records to law enforcement agencies, private litigants, and others who may have an interest in the records for different purposes. One statute that establishes a certificate program is 42 U.S.C. § 241. Other statutory certificate of confidentiality programs may also be available to CMS data users.
2. A certificate provides an extra layer of protection for the privacy interest of data subjects that is not readily available through other means. We recommend that all researchers, whether in federal agencies or other organizations, who seek identifiable or potentially identifiable data from CMS be required to obtain a certificate of confidentiality or to explain (preferably in a public document) why a certificate is not available.
3. We further recommend that the CMS data use agreement be amended to provide expressly that the data subjects of any data disclosed under the agreement are third party beneficiaries of the agreement. By so providing, the agreement will enhance the accountability of the researcher and may allow an aggrieved data subject to seek relief if his or her data is misused or improperly disclosed. The criminal penalties cited in paragraph 15 of the standard CMS data use agreement are useful but not sufficient. A data spill or other action by a researcher that harms a data subject may or may not rise to the level of criminality. Further, the willingness of the government to pursue criminal penalties even when available or appropriate is always uncertain. Providing for the possibility of a private remedy (if available under the law of the jurisdiction in question) enhances the relief that a data subject can pursue without the need for the approval of a government prosecutor.
4. In offering these comments on the CMS data use agreement, we want to note that we have not fully reviewed the agreement. Our comments here should not be construed as approval of the other provisions. It would be useful for CMS to independently seek public comment on its data use agreement.

V. Regulatory Impact Statement

The proposed rule does not include a regulatory impact assessment. The justification states:

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and

safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects (\$100 million or more in any 1 year). Neither plan sponsors nor pharmacies are required to perform any new task or purchase any new equipment or increase their labor force. This proposed rule does not reach the economic threshold and thus is not considered a major rule.

We believe that the judgment that the proposed rule is not economically significant is wrong. Even if it is true that no new tasks, equipment costs, or labor costs are imposed on sponsors or pharmacies, the costs and benefits of the proposed rule far exceed the \$100 million threshold and require a regulatory impact analysis. CMS reached its conclusion about costs and benefits without undertaking a fair or comprehensive assessment of costs and benefits from the proposed rule.

The proposed rule will result in the use and sharing of sensitive health information about millions of Americans. The value of the information on millions of drug recipients should have been estimated as a starting point for the analysis because it is a proxy for the costs imposed on data subjects. Personal information has a value in the marketplace, and it is possible to determine a value using this crude market measure. We can begin the exercise by offering an example of the type of analysis that CMS should have undertaken.

Data and list brokers rent information about individuals by health condition.¹ If we assume that there are an average of five data elements about the prescription drugs taken by 10 million individuals, then there are 50 million data elements. Mailing lists often rent for 10 cents a name. A list that reveals the prescription drug purchases, even with nothing more than name, address, and prescription drug, would be far more valuable. However, even the ten cents a name value produces a value of \$5 million dollars, and the list might rent multiple times a year. This represents a good percentage of the \$100 million threshold that would require a regulatory analysis. Adding in the value of information on the prescribing habits of physicians will further increase the total value of the information in the database. You can measure that value by looking at the profit statements of the commercial companies that traffic in physician data. Overall, we estimate that just the commercial value of the data in the Part D database exceeds the threshold. The marketplace value of the information is one measure of the economically significant effects of the proposed rule.

However, that only begins the economic analysis. A regulatory impact analysis must also consider the value of costs and benefits that cannot be measured in monetary units. The privacy consequences of the data sharing activities that the proposed rule would allow must also be assessed. It is difficult to put a dollar value on privacy, but the widespread sharing of data that CMS proposes will affect the privacy of every individual in the database. We know that many individuals value privacy highly. Some value their privacy so highly that they pay for health care costs out-of-pocket rather than report their treatments to insurers. This is one limited measure of the value of health privacy, and we believe that it is susceptible to measurement.

¹ For example, as of December 12, 2006, Walter Karl offered an "Ailment Sufferers Database" (list ID 108171) of 3,129,351 individuals with ailments such as asthma, diabetes, frequent headaches, Parkinson's Disease, and a host of other ailments. For more information, see <www.walterkarl.com>. Also, see Appendix A attached to these comments to see a screen shot of the data card on this list, current as of December 12, 2006.

We can create a broader measure with some reasonable assumptions. If we assume that Part D beneficiaries value their privacy at an average of only ten dollars a year, the value of privacy will exceed the threshold if there are only 10 million beneficiaries. If there are twenty million beneficiaries, we reach the threshold if privacy is valued at only five dollars a year.

Considering the risk that data sharing will increase the threat of a data breach offers another measure. Assume that there is a five percent chance of a data breach as a result of the significant amounts of data sharing that the proposed rule contemplates. Assume further that a data breach will require the purchase of credit monitoring for the data breach subjects (a common remedy paid for by the person responsible for the breach). Credit monitoring for one year for ten million individuals would cost several hundred million dollars. If the risk is five percent, this adds another possible ten or twenty million dollars in costs.

We can continue this preliminary assessment by considering the value of the activities for which the data is proposed to be shared. These activities involve costs that need to be assessed. The envisioned data transfers will result in the expenditure of government and other funds, and these are costs that must be considered. The costs may be outweighed by the resulting benefits. We think that CMS is in a far better position to estimate the potential costs and benefits of the research and administrative activities described in the proposed rule.

The overall point should be clear: CMS did not make any attempt to identify and assess all of the costs and benefits that may result from the proposed data sharing. We believe that it is crucial that privacy consequences of any proposed use or disclosure of personal information be included in any regulatory analysis. The difficulty of monetizing privacy costs should not be a barrier to attempting to place an appropriate dollar value for regulatory purposes. Failure to consider privacy leaves program beneficiaries to bear the costs and consequences of data sharing without those costs and consequences being considered to determine if the proposed activities are justifiable from an economic perspective.

CMS's failure to perform a regulatory analysis is a fatal flaw for the proposed rule. We believe that CMS must perform an analysis and republish the rule again for public comment.

VI. Other issues

A. HIPAA

HIPAA applies to Part D drug plans. However, the proposed rule does not explain why the Department has chosen to deny the applicability of HIPAA to CMS Part D activities when HIPAA applies to CMS activities for Parts A & B of Medicare. The proposed rule has only one brief mention of HIPAA, and that statement does not explain why HIPAA does not apply. An explanation would not only have been helpful, but it would have exposed the more precarious state of the privacy of Part D information in the possession of CMS.

Further, we believe that regardless of the technical applicability of HIPAA to Part D, the Department has made a poor choice in not applying HIPAA to CMS's Part D data activities. The

Department has the administrative capability to extend HIPAA to Part D. By having different privacy rules applicable to different parts of Medicare, the Department is making it more complex, difficult, and confusing for Medicare beneficiaries to understand and exercise their privacy rights. Another effect is a likely increase in confusion within CMS as employees struggle with patient data subject to differing privacy regimes.

We also observe that protections of the HIPAA security rule will not apply, and that this too raises costs and undermines patient protections. A recent GAO report found serious problems with security controls at CMS. See *Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network* (GAO-06-750) (Oct. 3, 2006).

More broadly, the Department's failure to apply HIPAA makes CMS's Part D operations the second major health data intensive activity within the Department of Health and Human Services to which the Department has avoided application of HIPAA. The other activity is treatment programs of the National Institutes of Health. While both conclusions may be technically correct under the currently defined scope of HIPAA, it would be simple for the Department to reach a different, fairer, and better result by adjusting the HIPAA rules to include these activities. By evading the application of HIPAA to these two health data intensive activities, the Department undermines public confidence in the operation of these two health programs and raises question whether the Department truly values the privacy and security protections of HIPAA. The protections of HIPAA should be available to patients at NIH and to beneficiaries of Part D whose data is in the possession of CMS.

B. Privacy Impact Assessment

The data activities that CMS proposes require the completion of a privacy impact assessment (PIA). OMB guidance on the E-Government Act of 2002 says that an agency must undertake a PIA "where a system change creates new privacy risks." There is no doubt that the proposed rule creates new privacy risks through the widespread sharing of data about drug recipients under Part D.

We see no evidence that CMS has conducted or plans to conduct a PIA. We believe that a PIA is required before the proposed rule can be implemented. We ask that CMS prepare a PIA, publish the PIA for public comment, and consider the comments before proceeding with the proposed rule.

C. Shortcomings of the Data

We do not have a clear understanding of the full scope of the data being collected. However, we can see some major shortcomings that may make the data far less useful than the proposed rule suggests for the many purposes that CMS envisions. We think that the data will likely turn out to be significantly incomplete and may not provide results that are useful or reliable. This in turn suggests that the conclusions that CMS wants to derive from the data may not be valid. If so, then there may well be no good reason to risk the privacy interests of beneficiaries in pursuit of flawed research and analysis.

Data may be missing from the database when drugs are paid for by wholly private health plans. Information on prescription drug use and purchase may also be missing for those who fall within the so-called donut hole in Part D. The proposed rule fails to recognize these potential shortcomings or to acknowledge that the data gaps will make it more difficult to achieve the benefits that the proposed rule contemplates. Further data problems may arise if the Part D program is subject to fraud or medical identity theft. Given the current rate of fraud in other CMS programs, then it stands to reason that Part D will also suffer from similar fraud issues, which will have a cumulative impact on data quality.

If flaws and gaps in the data make it impossible to reach valid conclusions, then the entire exercise may be pointless. Until CMS explains in more detail what data will be collected, what data won't be available, and what data may be useless because of fraud or other flaws, it is impossible to assess the value of the uses to which CMS expects to put the data.

Potential problems with the data are extremely important. CMS's basic argument that it must ignore the congressional data restrictions in order to find facts and reach conclusions about other matters. If the data's flaws are too great to achieve CMS's goals, then the purported justification for ignoring the data restrictions is undermined, perhaps fatally.

VII. Conclusion

CMS needs to do more to explain its plans for greater use of sensitive patient data and all of the possible alternatives to those plans before it can fairly ask for public comment on the proposed rule. Further, the public needs to see a draft Privacy Act system of records notice, including proposed routine uses, a Privacy Impact Assessment, and a Regulatory Impact Statement. Seeking public comment on the proposed rule without offering more information to the public is simply inappropriate.

We ask that CMS cancel the proposed rule, provide the additional information needed, and then publish another rule for comment.

We thank you for the opportunity to submit these comments.

Pam Dixon

Executive Director,
World Privacy Forum

Attachment: Appendix A

Appendix A

Direct Listline/ListFinder

12/12/2006 11:01 AM



Advertising | Contact Us | Multichannel Merchant Magazine | DM Buyer's Guide | E-Newsletters | Subscribe

Case Histories / Q&As | Exclusive Content | Legal/Regulatory | DM Disciplines | Opinions/Columnists | Resource Center | Events

December 12 2006

search advanced search



asthma

- All -

Find Lists

AILMENT SUFFERERS DATABASE

List ID 108171

SEGMENTS

3,129,351 Total Universe / Base Rate	\$105.00/M
Counts through 07/03/2006	
3,129,351 Total Database	\$105.00/M
219,005 Last 6 months	+ \$5.00/M

CONTACT

To obtain more information on this list, contact your List Broker

-- OR --

Lori Colantuono

Walter Karl
One Blue Hill Plaza
Pearl River, NY 10965

845 732-7089

FAX: 845 620-1885

lori.colantuono@walterkarl.infousa.com
www.walterkarl.com

-- OR --

[Click here to request information or a quote directly from the list manager.](#)

DESCRIPTION

Target a very specific audience of people who suffer from very specific medical problems. Additional Selection: Ailment @ \$40/M Ailments: Allergies 2,326,559 Alzheimer's 43,099 Angina/Heart Disease 262,794 Arthritis/Rheumatism 751,452 Asthma 925,021 Blindness/Visual Impairment 144,257 Diabetes 531,136 Eczema 128,477 Emphysema 85,230 Enlarged Prostate 44,505 Epilepsy 34,464 Estrogen 180,902 Frequent Headaches 547,526 Gastritis 175,502 Gingivitis 200,191 Hearing Difficulty 462,641 Heartburn 514,773 High Blood Pressure 1,002,429 High Cholesterol 784,318 Lactose Intolerant 188,267 Migraines 918,345 Osteoporosis 148,005 Parkinson's Disease 11,086 Physical Handicap 169,654 Sensitive Skin 545,201 Sinusitis 510,709 Sports Injury 195,764 Thinning Hair/Bald 453,369 Ulcer 147,831

powered by NextMark

[Terms of Use](#)

Browse E-Newsletters

DIRECTnewsline

DIRECTlistline

SearchLine

DIRECTTips