Comments of the World Privacy Forum

Regarding *Performance Measurement and Reporting System (PMRS)*, System No. 09-70-0584 to:

CMS Privacy Officer
Division of Privacy Compliance, Enterprise Architecture and Strategy Group
Office of Information Services
CMS
Room N2-04-27
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Via overnight mail

Re: *Performance Measurement and Reporting System (PMRS)*, System No. 09-70-0584, 72 Federal Register 52133-40

October 2, 2007

The World Privacy Forum offers comments on the proposal by the Centers for Medicare & Medicaid Services to establish a new system of records titled *Performance Measurement and Reporting System (PMRS)*, System No. 09-70-0584. The notice appeared in the Federal Register on September 12, 2007. 72 Federal Register 52133-40, <http://edocket.access.gpo.gov/2007/E7-17907.htm>.

The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to health care. See www.worldprivacyforum.org.

We are sympathetic with the primary purpose of this system of records, which is to "provide transparency in health care on a broad-scale enabling consumers to compare the quality and price of health care services so that they can make informed choices among individual physicians, practitioners and providers of services." However, we have profound concerns about the widespread disclosure of protected health information (PHI) – personally identifiable patient information as defined in the HIPAA health privacy rule – for this purpose. These comments focus exclusively on PHI and do not address the disclosure of information that identifies health care providers.

The stakes for individuals in this system of records are very high. The proposed system of records will contain information on every Medicare beneficiary. This is not a trivial matter. The CMS Medicare beneficiary data is a collection of medical information unmatched in the files of any other health care provider. CMS needs to be as careful as possible to ensure that the terms of any disclosures are drafted carefully and narrowly, and that every possible privacy protection has been incorporated. We are unconvinced that CMS recognizes the breadth or consequences of the disclosures that its notice would allow. The proposed system notice is sloppily written, poorly conceived, and of questionable legality.

In 2006, the World Privacy Forum released the first report on medical identity theft. Medical identity theft is a major activity that affects large numbers of individuals, costs Medicare and private insurers huge sums of money, and threatens the privacy and health treatment of victims. Medicare recipients are already the targets of thieves operating medical identity theft schemes, but the scope of this activity pales in comparison to what could be done with an entire database. There is no doubt that the Medicare beneficiary database would be the crown jewels for anyone seeking to profit from medical identity theft. If the database were obtained in whole or in part by a medical identity theft enterprise, the consequences would be enormous. Millions of individuals could be affected, and Medicare funds could be drained in the billions. Criminals would have a huge incentive to place a confederate in any organization that obtains the Medicare database. Insider access is already a known and prevailing technique for obtaining names and Social Security Numbers of patients who can become victims of a criminal enterprise.

Frankly, we do not understand how CMS can consider disclosing PHI of Medicare beneficiaries in the proposed fashion and to a potentially wide variety of agencies, individuals, and organizations without complete assurance that the data will be protected against any possible misuse. We do not think that the disclosures proposed in the PMRS system of records address security in any meaningful way. We are not convinced that any readily available security measures will protect the Medicare beneficiary database if it is handed out to agencies, individuals, and organizations as proposed in the system notice.

To be blunt about it, if CMS actions or inactions allow the data in this system to be misused, to leak out, or to be the subject of a security breach, the monetary cost to the government could be enormous, the privacy consequences for Medicare beneficiaries could be massive, and the political consequences for CMS and its senior officials could be lethal. One mistake by one recipient could create the largest and most legendary health privacy horror story ever. In short, whatever the benefits of disclosure of PHI from the PMRS system of records, the benefits do not and cannot outweigh the risks.

I. Legal Need for a Privacy Impact Assessment

Initially, we do not see any evidence that CMS has prepared a Privacy Impact Assessment (PIA) for this system of records. The size, scope, and consequences of this system are so vast that a PIA is both essential and legally required. The proposed system is new, will entail significant additional processing (including disclosures) of existing data, involves new interagency uses, and creates new privacy risks. See OMB Guidance for Implementing the Privacy Provisions of the E-

Government Act of 2002 (M-03-22) (2003),
<http://www.whitehouse.gov/omb/memoranda/m03-22.html.>

The PIA should provide a complete evaluation of alternatives to the disclosure of PHI, including the use of encryption and aggregation techniques that could make data available in useful formats without actually identifying individual patients. Concerns about disclosure of PHI would diminish if CMS itself conducted some or all of the data linkage and only released aggregate data or deidentified for additional analysis by other organizations. The need for a review of ways to limit the sharing of identifiable patient data is great because restricting identifiers may be the best way to accomplish the purpose of the system while protecting patient privacy. Other measures that need to be considered include: 1) establishing technical and administrative standards, including security, for any organization that seeks to obtain PHI from the proposed system of records; 2) requiring regular independent audits of any organization that obtains PHI, with full public reporting of the audit results; 3) publication of the methodology used by organizations undertaking transparency activities; 4) legal protections against compelled disclosure of any PHI in the hands of recipients undertaking transparency activities (e.g., such as the protections provided by certificates of confidentiality under 42 U.S.C. 241(d) and other statutes); and 5) establishment of a statistical enclave that would completely protect PHI from any possible secondary use.

The World Privacy Forum recommends that a PIA should be prepared *and published as a draft document for public comment* before proceeding further with the system of records notice. After final publication of a PIA, the system notice should be revised and republished for public comment.

II. Conditions for Disclosures

Routine uses 4 and 6 include a set of conditions that apply to disclosures. The conditions are similar but not identical. Routine use 4 (Chartered Value Exchanges and data aggregators) calls for these determinations by CMS:

> a. Determines that the use or disclosure does not violate legal limitations under which the record was provided, collected, or obtained;
> b. Determines that the purpose for which the disclosure is to be made:
> (1) Is of sufficient importance to warrant the effect on and/or risk to the privacy of the individual that additional exposure of the record might bring, and
> (2) There is reasonable probability that the objective for the use would be accomplished;
> c. Requires the recipient of the information to establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record,
> d. Make no further use or disclosure of the record except:
> (1) For use in another project providing transparency in health care, under these same conditions, and with written authorization of CMS;
> (2) When required by law.

e. Secures a written statement attesting to the information recipient's understanding of and willingness to abide by these provisions. CVEs and data aggregators should complete a Data Use Agreement (CMS Form 0235) in accordance with current CMS policies.

Routine use 6 (individual or organization with projects that provide transparency in health care) provides for these CMS determinations:

a. Determines that the use or disclosure does not violate legal limitations under which the record was provided, collected, or obtained;
b. Determines that the purpose for which the disclosure is to be made:
(1) Cannot be reasonably accomplished unless the record is provided in individually identifiable form,
(2) Is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring, and
(3) There is reasonable probability that the objective for the use would be accomplished;
c. Requires the recipient of the information to:
(1) Establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, and
(2) Remove or destroy the information that allows the individual to be identified at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the project, unless the recipient presents an adequate justification of a research or health nature for retaining such information, and
(3) Make no further use or disclosure of the record except:
(a) For disclosure to a properly identified person, for purposes of providing transparency in health care enabling consumers to compare the quality and price of health care services so that they can make informed choices among individual physicians, practitioners and providers of services;
(b) In emergency circumstances affecting the health or safety of any individual;
(c) For use in another research project, under these same conditions, and with written authorization of CMS;
(d) For disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit; or
(e) When required by law.
d. Secures a written statement attesting to the information recipient's understanding of and willingness to abide by these provisions. Researchers should complete a Data Use Agreement (CMS Form 0235) in accordance with current CMS policies.

Some of these conditions are the same, but some are not. We do not understand how CMS selected the conditions for these routine uses.

• Routine use 6 allows disclosure only if there is a finding that the disclosure "cannot be reasonably accomplished unless the record is provided in individually identifiable form." We see no reason why that same determination should not be required for disclosures under routine use 4. Without that same condition, disclosures of identifiable information would be possible under routine use 4 even if the purposes of the disclosure could be accomplished without identifiable data. If there is any justification for disclosing identifiable data when the identifiers are not needed, it is not apparent from the notice or otherwise.

• Routine use 6 requires the recipient to "remove or destroy the information that allows the individual to be identified at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the project, unless the recipient presents an adequate justification of a research or health nature for retaining such information". There is no comparable requirement for routine use 4. We do not understand why the condition is absent. If there is no reason for retention of identifiers, then identifiers should be deleted. This is as basic a privacy principle as there is. We note that the condition itself already recognizes the possibility that there could be adequate justification for retaining identifiers, so we are even further mystified at the absence of any requirement to remove or destroy identifiers.

• Routine use 4 prohibits redisclosure by the recipient except:

(1) For use in another project providing transparency in health care, under these same conditions, and with written authorization of CMS;
(2) When required by law.

But routine use 6 allows more redisclosures by the recipient, namely these five exceptions:

(a) For disclosure to a properly identified person, for purposes of providing transparency in health care enabling consumers to compare the quality and price of health care services so that they can make informed choices among individual physicians, practitioners and providers of services;
(b) In emergency circumstances affecting the health or safety of any individual;
(c) For use in another research project, under these same conditions, and with written authorization of CMS;
(d) For disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit; or
(e) When required by law.

We much prefer the narrower limits in routine use 4. We have no objection to disclosures required by law in either routine use.

We do not understand why emergency circumstances might justify disclosure under routine use 6 but not 4. Nevertheless, we would prefer to drop this routine use entirely. The Privacy Act already has a statutory condition of disclosure at 5 U.S.C. § 552a(b)(8) that is sufficient to cover any emergency disclosure affecting health or safety. We also note that the routine use does not

include the statutory requirement that the subject of a record be notified of any emergency disclosure. If the routine use seeks to vary the standard or procedure specified in the statute, the routine use is improper. If the routine use does not vary the standard or procedure specified in the statute, then it is unnecessary.

We object to routine use 6 redisclosures to another person undertaking transparency activities. The routine use (which we will discuss more substantively later) allows disclosure to "individuals and organizations." It is not clear that these recipients must be researchers. We see no requirement for approval of a research project by an IRB. We see no requirement that the recipient qualify as a researcher. The words are "individual and organizations" and not "researchers." We find the routine use itself to be ambiguous on this point.

However, we see no reason why one recipient of PHI should be allowed to make a disclosure of that PHI to any other person who glows with the same transparency intent subject only to the condition that the person be "properly identified." It isn't even clear that the subsequent requirement in the routine use that CMS obtain "a written statement attesting to the information recipient's understanding of and willingness to abide by these provisions" applies to subsequent recipients. However, the notion that one organization can give PHI to another, and that the second organization can pass it on to yet a third, and so on ad infinitum is so outrageous as to not require any extended discussion. The possibility of secondary, tertiary, and additional disclosures is a major loophole.

In contrast, routine use 4 allows redisclosure "for use in another project providing transparency in health care, under these same conditions, and with written authorization of CMS." We do not understand why these comparable provisions in routine uses 4 and 6 are different. We do not understand why written authorization of CMS is not included in the routine use 6 redisclosure provision.

The best result here would be to drop the redisclosure authority entirely for other transparency projects. It potentially opens the floodgates and allows all individually identifiable Medicare patient information to be passed around with no oversight, few meaningful controls, and no hope of enforcement by CMS, patients, or any other aggrieved individual. If a recipient violates the rules and hands the data over to a credit bureau, bank, or data broker – or places the data on the Internet – the privacy of Medicare beneficiaries will be irretrievably lost and beneficiaries will have no way to recover their privacy even if there are legal remedies. If there is any justification for these secondary disclosures – and we doubt that there is – CMS should play a direct role in the decision to disclose and in establishing the conditions for disclosure.

We are not finished discussing the conditions for disclosures. As we just pointed out, routine uses 4 and 6 include conditions applicable to recipients. We see no comparable conditions for disclosures under routine use 2 (other federal or state agencies or "an agency established by state law"). Why should PHI be given to these agencies without any restrictions on how the data will be used, redisclosed, and destroyed? Are these recipients exempt from the possibility that they might misuse the data or fail to protect it? Should they be allowed unlimited secondary uses? The routine use says that the disclosures will be pursuant to agreements with CMS, but we do not

know what those conditions will be. Just as with routine uses 4 and 6, the conditions should be spelled out in the published routine use and not left subject to the whim of CMS employees.

We make the same point about the lack of conditions governing disclosures for routine use 5 (to assist individual physicians, practitioners, providers of services, suppliers, laboratories, and other health care professionals who are participating in health care transparency projects). We see no reason why these disclosures of PHI should be free of conditions.

We make the same point about the lack of conditions governing disclosures for routine use 7 (Quality Improvement Organizations). We see no reasons why these disclosures of PHI should be free of conditions.

We do not make the same point about the lack of conditions governing disclosures for routine use 8 (Department of Justice). Some litigation disclosures to the Department of Justice to assist CMS qualify as disclosures for health care operations and should be subject to a business associate agreement. That agreement will restrict the use of PHI by the Department of Justice, as will Executive Order 13181 (To Protect the Privacy of Protected Health Information in Oversight Investigations). It would be appropriate for the routine use to refer to the requirement for a business associate agreement prior to these disclosures.

Other possible litigation disclosures will be subject to the conditions established in 45 CFR 164.512(e). CMS is not likely to be able to place conditions on these disclosures. To the extent that routine use 8 suggests that disclosures can be made under circumstances not allowed by HIPAA, the routine use may be overbroad and therefore improper. We address this point about the interplay between routine uses and HIPAA later in these comments.

Routine use 9 (CMS contractors) includes some conditions on disclosure. These disclosures will be subject to business associate agreements, although the routine use fails to mention business associate agreements. The discussion elsewhere in the notice – but not the routine use itself – suggests that agreements will prohibit contractors from "using or disclosing the information for any purpose other than that described in the contract" and will require the contractor "to return or destroy all information." Those conditions should be spelled out in routine use 9, just as they are with routine use 4 and 6.

We make the same point about the lack of conditions on disclosures made under routine use 10 (agencies engaged in fraud, waste, and abuse investigations). Disclosures for the stated purposes may be reasonable, but the absence of any conditions on use or redisclosure is striking, unfortunate, and inappropriate. We accept the need for disclosures for these investigations, but further secondary uses should be expressly prohibited.

Finally, we observe generally that the disparate treatment of disclosure conditions in the various routine uses is hard to understand. We do not understand why some routine uses have restrictions within the routine use; why some restrictions are mentioned in the discussion but not in the actual routine use; and why some routine uses have no restrictions on subsequent processing at all. Our guess is that the routine uses were cobbled together from existing routine uses in other CMS systems of records, and that many of those routine uses were written before the HIPAA

privacy rule took effect. CMS may need to review and revise all of its routine uses governing identifiable patient information to reflect the new (or not-so-new) HIPAA environment.

III. Limits Imposed by HIPAA

The system notice includes this general recognition of the limits imposed by the HIPAA privacy rule:

> Additional Circumstances Affecting Routine Use Disclosures. To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR Parts 160 and 164, Subparts A and E) 65 Fed. Reg. 82462 (12-28-00). Disclosures of such PHI that are otherwise authorized by these routine uses may only be made if, and as, permitted or required by the ``Standards for Privacy of Individually Identifiable Health Information." (See 45 CFR 164-512(a)(1)).

We do not believe that it is proper for CMS to propose routine uses that purport on their face to allow illegal disclosures. If a disclosure is not permitted by HIPAA, then a routine use that allows that disclosure cannot be lawfully promulgated. Adding a general limitation recognizing HIPAA's restrictions does not inform the public (or CMS staff) about the range of possible disclosures does not cure the defect.

We take routine use 6 as an example to make the point. The first part of the routine use authorizes disclosure:

> To assist an individual or organization with projects that provide transparency in health care on a broad scale, enabling consumers to compare the quality and price of health care services; or for research, evaluation, and epidemiological projects related to the prevention of disease or disability; restoration or maintenance of health or for payment purposes if CMS:
>
> a. Determines that the use or disclosure does not violate legal limitations under which the record was provided, collected, or obtained;

After some study of HIPAA, we cannot determine whether a disclosure of PHI for this purpose is lawful under HIPAA. It is far from clear that a disclosure to this class of recipients for the stated purpose qualifies as a health care operation, public health activity, or health oversight activity. These are the only provisions in HIPAA that appear to support any argument justifying the disclosure, and we have our doubts that transparency disclosures can be made under any of these provisions.

If CMS believes that it has authority under HIPAA to make the disclosures permitted under routine use 6, then it has an obligation to the public to explain. It is inappropriate at best and improper at worse to propose an expansive routine use that allows the disclosure of PHI to any "individual or organization" with a general disclaimer that no disclosures that violate HIPAA will be made. The public has no way to evaluate the routine use without substantial expertise in HIPAA. Frankly, even those with expertise in HIPAA may be mystified about the scope of

legally permissible disclosures under the routine use. Under our reading of HIPAA, none of the disclosures for transparency purposes under routine use 6 is lawful.

If all disclosures were made using business associate agreements, then there would be greater potential for specific privacy and security controls and for express limitations on secondary use and disclosure of PHI. However, it is not clear to us that all of the proposed disclosures could be made in that fashion. We cannot determine if CMS has the authority under HIPAA to disclose its entire beneficiary database to all the disparate recipients envisioned by the routine uses even under business associate agreements.

We observe that routine use 6 may be so broad as to permit a health care provider to contact a named patient with the information that the provider's death rate or price is lower than that of the patient's current provider for the patient's specific condition. We believe that everyone would find this activity to be improper, offensive, and violative of privacy, and we do not think that CMS intends recipients to use the data in this manner. However, we do not find anything in the routine use itself that would prevent use of the information for individual rather than aggregate activities. The words *broad scale* hint at limits on use of the transparency data, but the words impose no clear restriction.

CMS has an obligation to explain how each routine use is consistent with the authority in the HIPAA privacy rule. If a routine use allows disclosures that are broader than those permitted by HIPAA, then the routine use must be narrowed so that it is consistent with HIPAA. We recognize that there may be some disclosures that can only be properly assessed under HIPAA (or under the Privacy Act of 1974 itself) in context and with the facts relevant to the specific disclosure. Revised routine uses can accommodate the need to consider the circumstances of a specific disclosure at the time when the disclosure is under consideration. However, a routine use that allows a disclosure that is always prohibited by law cannot be proper.

A routine use might say, for example, that a disclosure to a class of recipients will only be made if consistent with the substantive and procedural requirements of the health oversight activities provision of HIPAA. A routine use with that degree of specificity would inform the public of CMS's view of the legal basis for the disclosure and would reference any additional limitations and prerequisites for the disclosure. Unless routines uses for PHI are tied to HIPAA disclosure authority, the public cannot assess what disclosures may or may not be lawful. This is the basis for our conclusion that the system of records notice itself is incomplete and may be legally insufficient.

IV. Comments on Specific Routine Uses

Routine Use 1 (To support Agency contractors)

We have no objection to this routine use. However, we note that the limits and procedures mentioned in Part III of the notice are not included in the routine use itself. This is a poor choice. Once published in its final form, the explanatory text accompanying the system notice will be forgotten, and those who read the routine uses will only see the text in the system notice. We recommend that the routine use be amended to mention the "safeguards are provided in the

contract/similar agreement prohibiting the contractor, consultant, or grantee from using or disclosing the information for any purpose other than that described in the contract/similar agreement and requires the contractor, consultant, or grantee to return or destroy all information at the completion of the contract."

This comment applies to all routine uses. Any limitation, procedure, or restriction mentioned in Part III or other parts of the notice should be included in the text of the routine uses. All routine uses require greater specificity.

Routine Use 2 (Federal or State agencies)

The routine use would allow disclosure of PHI to a "state agency, agency of a state government, or an agency established by state law." We do not understand the difference between these three categories of state agencies. Frankly, we wonder if the verbiage is covering the possibility of the disclosure of patient information to a private entity established under state law. We need to know more about the range of possible recipients in order to understand the risks and legality of disclosures. This need is great because the disclosures under this routine use have no conditions that limit use, restrict disclosure, or require removal or destruction of identifiers. We foresee the possibility that Medicare beneficiary records could be disclosed to a private/public entity of a state and then reused for another purpose, disclosed to additional recipients, or even posted on the Internet.

Routine Use 3 (assist in making the individual physician-level performance measurement results)

This routine use is broad, vague, and unqualified, and we repeat the full text here:

> To assist in making the individual physician-level performance measurement results available to Medicare beneficiaries, through a Web site and other forms of data dissemination, in order to promote more informed choices by Medicare beneficiaries among their Medicare coverage options.

The routine use fails the first test for routine uses. It does not identify who the recipients of the data may be. As written, anyone in the world could be a recipient of individual physician-level performance measurement results. If there were no possibility that individually identifiable patient data were covered by this routine use, we would not be as concerned. However, nothing in the routine use suggests that it does not allow the disclosure of PHI. If CMS wants to make physician data available to the world, we have no privacy objection. That isn't what the routine use says. It would allow disclosure to anyone "to assist" in making physician results available. Would PHI disclosures "assist" in accomplishing that goal? We recommend that the disclosure of PHI under this routine use be expressly prohibited and that the range of recipients be clarified.

Routine Use 4 (Chartered Value Exchanges and data aggregators)

We have already discussed this routine use in Part II of these comments regarding conditions for disclosures. We offer an additional observation. The routine use does not explain who qualifies as a *data aggregator*. Might it include a data broker (e.g., ChoicePoint) or a credit bureau (e.g.,

Equifax)? We observe that the selection of a data aggregator to process PHI must be undertaken with great care. The entire transparency program could be terminated by a headline that says: "CMS Disclosures all Medicare Beneficiary Data to ChoicePoint."

The notice states elsewhere that "CMS also may provide physician and patient identifiable protected health claims data information to *data aggregators that are HIPAA business associates* of CMS (including working with providers, payers, or other HIPAA covered entities) for purposes for generating these results." (emphasis supplied). But nothing in the routine use suggest any limitation or procedure applicable to data aggregators. We recommend that the text of the routine use be amended to define, limit, and tie the concept of *data aggregators* to business associate requirements. We also think that the qualifications of data aggregators be specified in the routine use to exclude any entity that sells other consumer data for any general business, credit, identification, or marketing purpose.

Routine Use 5 (to assist health care professionals)

This routine use allows disclosure:

> To assist individual physicians, practitioners, providers of services, suppliers, laboratories, and other health care professionals who are participating in health care transparency projects.

This is another unqualified routine use that seemingly permits the disclosure of all Medicare beneficiary information to anyone is the world who may be assisting in a transparency project. The lack of qualification and specificity makes the routine use legally questionable.

Elsewhere, the notice states:

> PMRS data will be released to the individual physician only on those individuals who received services ordered or provided by the individual physician and shall be limited to claims and utilization data necessary to perform that specific project function whose information was provided for the PMRS project. Individual physicians, practitioners, providers of services, suppliers, laboratories, and other health care professionals require PMRS information for the purpose of direct feedback with respect to their individual patients on a non-aggregated basis.

We do not see anything in the routine use that states that disclosures will be limited to an individual physician and only about those individuals who received services ordered or provided by that physician. Some of the problems with the routine use would be cured if it included language to that effect.

The reference in the quoted language to *physicians* is curious. Is the intent to exclude all other health care providers? The second quoted sentence refers to other providers, but the first does not. We are mystified at the differences within this routine use.

That second sentence refers to health care professionals who require information "for the purpose of direct feedback with respect to their *individual patients on a non-aggregated basis*." (emphasis supplied). The intent and scope of that language is far from clear. Is this system to be used by CMS to tell individual physicians how they should treat individual patients? The role of CMS in overseeing the practice of medicine by individual practitioners is not within the zone of interest of the World Privacy Forum. However, we observe that the implications here are enormous and are not likely to be well received by providers or patients. Regardless of CMS's actual intent, the language needs to be clarified.

Routine Use 6 (assist an individual or organization with projects that provide transparency)

We repeat the first part of this routine use here:

> To assist an individual or organization with projects that provide transparency in health care on a broad scale, enabling consumers to compare the quality and price of health care services; or for research, evaluation, and epidemiological projects related to the prevention of disease or disability; restoration or maintenance of health or for payment purposes if CMS:****

First, we do not understand how to parse the sentence. The most likely reading is that the routine use covers three separate types of disclosure. The first is to individuals or organization undertaking transparency projects. The second is for research, evaluation, and epidemiological projects related to the prevention of disease or disability. The third is for restoration or maintenance of health or for payment purposes. We are not sure if that reading is correct, and we recommend that CMS clarify its intent. We also recommend if there are several different purposes covered by this routine use that they be broken out into separate routine uses.

We have already discussed the questions raised by limitations in the HIPAA privacy rule regarding disclosures for transparency purposes. We cannot find any clear authority in HIPAA for these disclosures. The problem is compounded by the phrase "individual or organization" in the first clause. The routine use suggests that disclosure could be made to any individual or organization, whether private or governmental, whether for profit or not-for-profit, whether domestic or foreign. Nothing in the routine use establishes standards, qualifications, or requirements for the person receiving the PHI for analysis. We have already discussed the inadequacies of the conditions established by routine use 6 setting standards for recipient processing. Even if those conditions are improved, they are not sufficient to support disclosure of PHI to any "individual or organization." Would CMS be willing to turn over the Medicare database to a newspaper? To a blogger? To a bank? To a tabloid newspaper? To a pharmaceutical manufacturer? To an employer? The scope of possible recipients is both broad and scary, and it is even harder to understand how any of the disclosures to these and other persons would be consistent with HIPAA. Even if the disclosures were legally permissible, it is hard to understand why CMS would be willing to disclose data to some of these potential recipients. We would be much happier seeing strict limitations in the routine use itself and not to have to hope that CMS will in the future exercise suitable discretion.

The second class of purposes for disclosure under routine use 6 – for research, evaluation, and epidemiological projects – is less controversial. However, it isn't clear what these three terms mean and how they differ. We have no idea what *evaluation* means. Is an *epidemiological project* something different from *research*? HIPAA defines research, but the suggestion of this routine use is evaluation and epidemiological projects are not research. That may not be the intent, but the confusion remains.

HIPAA allows disclosures for research under specified circumstances. We see nothing in the routine use that references these requirements or incorporates them as conditions for disclosure for these purposes. Would research disclosures be subject to the HIPAA conditions but not evaluation disclosures? It is impossible to interpret the routine use without definitions and more details.

The third category – restoration or maintenance of health or for payment purposes – is even more troublesome. Does CMS propose to disclose information about some or all Medicare beneficiaries to someone – it isn't clear whom the class of intended recipients could be – to restore or maintain the health of an individual? The potential scope of the disclosures under this authority is both breathtaking and terrifying. Will CMS disclose information about one beneficiary to a physician selected by CMS with the goal of having that physician intervene without other invitation to restore or maintain the beneficiary's health? Will CMS disclose a patient's PHI to a pharmaceutical manufacturer to allow the manufacturer to market a drug to the patient that CMS think will improve health? Will CMS disclose information to an employer to pressure an employee to undertake a treatment that CMS thinks would be beneficial?

The preamble to routine use 6 is hard to parse, hard to understand, and hard to accept. Its terms are undefined, and the purposes are vague or overbroad. We cannot believe that CMS intends disclosures that are as diverse and unprecedented as our analysis suggests, but we see little in the current language to prevent the disclosures. We recommend that the routine use be scrapped and redrafted so that the authorized disclosures are clear and narrow, that the recipients are carefully qualified, and that the purposes of the disclosures are demonstrably legal.

Routine Uses 7 through 10

We have no comments on these routine uses beyond those already covered in Part II of these comments.

V. Substance Abuse Rules and Other Legal Restrictions

We do not normally subscribe to the view that some personal information, medical or otherwise, is more "sensitive" than other personal information. However, records of substance abuse treatment subject to the rules in 42 CFR Part 2 are protected by a set of privacy rules and disclosure restrictions that are much more rigorous than the protections in the HIPAA health privacy rule. We see nothing in the proposed system notice that addresses how the substance abuse rules will limit disclosures under the routine uses or how any possibly lawful recipients of substance abuse information will have to comply with the restrictions attach to secondary uses of the records. This is a significant problem with the notice – not only because it supports our view

that the routine uses are both too expansive and improper – but also because it may mislead CMS employees into treating substance abuse records in the proposed system under the same terms as other records. We believe that the notice needs to pay more attention here. While we question the adequacy of the notice language acknowledging the HIPAA restrictions on disclosures, we wonder why there have been no similar recognition of the substance abuse restrictions.

Finally, we note that some other categories of information in this system are subject to various state and perhaps federal privacy laws governing records about HIV/AIDS, psychiatric treatment, or genetic information. Whether those laws apply to CMS or not, the agency should take note that specific protection laws were enacted by the states with broad public support. The casual sharing of these records with new users is not likely to be well-received by the public.

VI. Conclusion

The World Privacy Forum is pleased to have the opportunity to comment on this proposed system of records. We reiterate that CMS needs to do a lot more work before this system notice can be published in final form. In general, CMS should: 1) complete and publish for comment a Privacy Impact Assessment; 2) revise, clarify, and narrow the routine uses; and 3) explain how disclosures of PHI can be done consistently with the HIPAA privacy rule.

We would like to suggest an alternate interim approach. Most of our objections to the system notice are diminished if the disclosure of PHI is not allowed. CMS should consider proceeding with some transparency activities while the questions about disclosure of PHI are explored. A shorter and simpler system notice that excludes the possibility of disclosure of PHI would draw fewer objections about the privacy of Medicare beneficiaries. The World Privacy Forum believes that this plan will eventually draw considerable attention from the public. In its current form, we expect that this plan will be seen by many as offering more risk than benefit.

Respectfully submitted,

/s/

Pam Dixon
World Privacy Forum
www.worldprivacyforum.org
760.436.2489