Comments of the World Privacy Forum

VIA EMAIL AND MAIL

June 14, 2006

CMS Privacy Officer,
Division of Privacy Compliance Data Development
CMS
Mail Stop N2-04-27
7500 Security Boulevard
Baltimore, Maryland 21244-1850.

Re: System of Records Notice for Medicaid Program and State Children's Health Insurance Program (SCHIP) Payment Error Rate Measurement (PERM), System No. 09-70-0578, 71 Fed. Reg. 28347-28351 (May 16 2006).

Pursuant to the notice published in the Federal Register on May 16, 2006 regarding the System of Records Notice ``Medicaid Program and State Children's Health Insurance Program (SCHIP) Payment Error Rate Measurement (PERM), System No. 09-70-0578, the World Privacy Forum respectfully submits the following comments.

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, including topics in medical privacy. We have been actively engaged in the area of medical privacy; we testified before The National Committee on Vital and Health Statistics (NCVHS) on the privacy and confidentiality of electronic health records and the proposed National Health Information Network, and recently, we published the first major report on medical identity theft.[1]

The Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS) published a System of Records Notice that includes a number of crucial routine uses. The World Privacy Forum requests that CMS amend the System of Records Notice to correct an oversight and to address other privacy-related issues in the notice.

[1] See <http://www.worldprivacyforum.org>.

I. The System of Records needs to reference Executive Order 13181.

The System of Records Notice for System No. 09-70-0578[2] does not reference Executive Order 13181 of December 20, 2000, "To Protect the Privacy of Protected Health Information in Oversight Investigations."[3] President Clinton signed this order when the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules were first published. Executive Order 13181 restricts law enforcement use of health records against individuals; specifically, it states:

> It is the policy of the Government of the United States that law enforcement may not use protected health information concerning an individual, discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations, against that individual except when the balance of relevant factors weighs clearly in favor of its use.[4]

At a minimum, the System of Records Notice should specifically reference Executive Order 13181. However, the better course of action would be to incorporate the substance of the policy reflected in the Executive Order directly in the routine use. The policy protecting individuals against the use of Protected Health Information (PHI) discovered during health oversight agencies should be stated as an express limitation on disclosures to other agencies for fraud investigations. CMS should make compliance with Executive Order 13181 a condition of any referral. We also observe that the policy of the Executive Order also applies to civil and administrative investigations and may impose limitations on internal CMS activities as well as investigations conducted with or by other agencies.

The failure to reference the order in this Systems of Records Notice is at best an oversight and at worst a failure to comply with the letter and/or spirit of Executive Order 13181.

II. CMS cannot define routine uses covering HIPAA records without taking into account in the text of the routine use the HIPAA requirements that significantly limit disclosure or that establish additional procedural requirements.

The CMS May 16 System of Records Notice says:

> B. Additional Provisions 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

---

[2] System of Records Notice for Medicaid Program and State Children's Health Insurance Program (SCHIP) Payment Error Rate Measurement (PERM), System No. 09-70-0578, 71 Fed. Reg. 28347-28351 (May 16 2006). Hereafter cited as 71 Fed. Reg. 28347-28351 (May 16 2006).

[3] Executive Order 13181. "To Protect the Privacy of Protected Health Information in Oversight Investigations." Signed December 20, 2000. See 65 FR 81321 (December 26, 2000). <http://www.archives.gov/federal-register/executive-orders/2000.html>.

[4] *Ibid.*

> and E) 65 FR 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)).[5]

While the thought expressed in this limitation is admirable as well as legally mandated, it is not enough to comply with both the Privacy Act of 1974 and the HIPAA health privacy rule. A routine use that on its face permits a disclosure that violates legally binding HIPAA standards is an improper routine use. An agency cannot describe a routine use that allows both legal and illegal disclosures and then say in another part of its notice that it will not make disclosures that are illegal. Each routine use must stand on its own and fully and clearly describe the extent to which disclosures are allowed. A routine use is not just authority for an agency to disclose. It is a public notice of the scope of authorized disclosures. This is why the law requires routine uses to be included on forms used to collect personal information. 5 U.S.C. §552a(e)(3)(C). A disclaimer included in another place is not legally sufficient.

Consider the third proposed routine use:

> 3. Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.
>
> Individuals sometimes request the help of a Member of Congress in resolving some issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.[6]

To the extent that this routine use covers disclosure of a HIPAA record, the disclosure would require a signed authorization by the constituent that meets the HIPAA standard. For the routine use to suggest that disclosure of a HIPAA record can be made on another basis is misleading to the public, to congressional staff and members, and to CMS staff.

In addition, it is worth noting that if an authorization for the disclosure has been obtained from the data subject, then no routine use is actually needed. The Privacy Act already allows disclosures with the "prior written consent" of the data subject.[7] Thus, a routine use that properly reflects the HIPAA requirements is at best superfluous and at worst improper. A routine use that duplicates the statutory disclosure authorization would be a nullity. If CMS sees the need for a routine use that covers only non-HIPAA records, that narrow routine use may meet legal standards.

---

[5] 71 Fed. Reg. 28347-28351 (May 16 2006).
[6] *Ibid.*
[7] "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions]." 5 U.S.C. § 552a(b).

Next consider the routine use that allows disclosures to agency contractors. If the records involved are HIPAA records, then a business associate agreement would be almost certainly be necessary. In addition HIPAA security requirements would also apply to the contractor and the transferred data. The same standard contractor routine use that may have been adequate before the HIPAA rules became effective no longer meets the legal requirements of the Privacy Act. A routine use should, in its own text, reflect the substantive and procedural limitations found in HIPAA.

Lastly, without making any attempt to be comprehensive in analyzing the proposed routine uses, we offer another example. The routine use for litigation fails to match up with the complex and explicit requirements in HIPAA.[8] Some litigation disclosures by CMS may qualify as health care operations, and the proposed routine use might be adequate for those litigation disclosures. We do not take a position on that narrow point. However, many other litigation disclosures can only be made with prerequisites clearly set out in the HIPAA privacy rule. Any routine use addressing those disclosures must do a better job of incorporating the HIPAA requirements in the text of the routine use.

In general, these shortcomings of the routine uses are not trivial. If CMS relies on a routine use that fails to meet Privacy Act standards for clarity and completeness, it runs the risk that all disclosures made on that basis of that routine use will be held to be illegal. The consequences of illegal disclosures could be stunning. Any further use of improperly disclosed information might be prohibited. The agency might be exposed to the possibility of paying actual damages to each individual whose record was disclosed. Legitimate criminal prosecutions could be endangered. There is no reason for CMS to take these risks.

We are not unaware of the likelihood that CMS, HHS, and many other government agencies that maintain HIPAA records in Privacy Act systems of records may have been following the same routine use policy and practice reflected in the notice in question here. Whether this has been the result of oversight, laziness, or a reasoned process is unknown to us. In our view, all routine uses covering HIPAA records should have been revised and republished to recognize HIPAA requirements.

At present, we request only that the routine uses for this system of records be revised to reflect the HIPAA requirements as appropriate when the disclosures involve HIPAA records. One possible approach may be to have separate routine uses for HIPAA records and for records in the system (if any) not subject to HIPAA.

We suggest, however, that CMS and HHS should consider undertaking the broader assignment of conforming all routine uses for records covered by HIPAA with the legal requirements that we have set out here. That task is large, but the risks of failure to meet the standards of the law are larger.

---

[8] 45 C.F.R. § 164.512(e).

III. Discussion of disclosure policy of directly identifiable data

The System of Records Notice says:

> In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).[9]

The World Privacy Forum supports the policy stated in the above paragraph. The policy could be improved by attention to the possibility that someone who is not "familiar with the enrollees" could also use the data and re-identify individuals. On this general point, we refer you to the Illinois Supreme Court's decision in Southern Illinoisan v. Illinois Department of Public Health, <http://www.state.il.us/court/opinions/SupremeCourt/2006/February/Opinions/Html/98712.htm>. In that case, an expert with no familiarity with the subjects of a disease registry was able to identify many of the individuals in the registry from very limited and seemingly non-identifiable information. We see no reason to limit the concern about re-identification to "those familiar with the enrollees."

We note that the issue raised by the quoted paragraph seems applicable more broadly to CMS data, and we wonder why there is not a broader CMS rule or policy addressing re-identification possibilities for de-identified data. The Privacy Act of 1974 only regulates the disclosure of identifiable records maintained in a system of records. The possibility that indirectly identifiable information specified in the System of Records Notice might be identifiable in some circumstances is a legitimate concern, but it is one that likely falls outside the scope of the Act. If that is the case, then we wonder about the legal significance of the policy in a Privacy Act system notice. We still support the general policy, with the modification suggested above, but there may be a more effective and more binding way for CMS to express its policy on re-identification.

As CMS is aware, HIPAA itself sets some standards for de-identification of PHI.[10] To the extent that the HIPAA requirements attach, there are already clear standards for the release of de-identified data, and those standards appear to be stated differently than the policy in the paragraph quoted above. Without knowing more about the facts of actual disclosures, we cannot assess the possibility that the CMS standard in this system of records may differ from the more detailed HIPAA standard.

---

[9] 71 Fed. Reg. 28347-28351 (May 16 2006).
[10] 45 C.F.R. § 164.514(a), (e).

Finally, we observe in passing that standards for identifiability under the Privacy Act of 1974 are, for the most part, unaddressed in the Act or related materials. Identifiability has over the years become a complex issue of law, statistics, and policy. We applaud CMS for raising the issue here, but we believe that there is a need for a broader approach to the problem. We stand ready to assist in helping to find that approach.

IV. Conclusion

The World Privacy Forum appreciates the opportunity to submit comments on this System of Records Notice.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
+1 760.436.2489