Comments of the World Privacy Forum to the Office for Civil Rights, Department of Health and Human Services regarding Request For Information: HIPAA Privacy Rule Accounting for Disclosures under HITECH Act, RIN 0991-AB62

Via regulations.gov

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Accounting of Disclosures
Hubert H. Humphrey Building
Room 509F
200 Independence Ave SW
Washington, DC 20201

May 18, 2010

The World Privacy Forum is pleased to have this opportunity to respond to the request of the Office for Civil Rights, Department of Health and Human Services, for information about the accounting for disclosures provisions of the HIPAA health privacy rule. The request appeared at 75 Federal Register 23214 (May 3, 2010), http://edocket.access.gpo.gov/2010/pdf/2010-10054.pdf.

The World Privacy Forum is a non-profit, non-partisan public interest research group that focuses on analysis and research of privacy issues, including issues relating to health care privacy. More information on our work may be found at http://www.worldprivacyforum.org.

We have responded to questions 1, 5, and 7 from the RFI, and we have included some additional thoughts on the issue at the conclusion of our comments.

1. What are the benefits to the individual of an accounting of disclosures, particularly of disclosures made for treatment, payment, and health care operations purposes?

Response: An individual cannot fully protect his/her privacy interest in a health record (and most other records) unless he/she has a right of access to the record, the right to propose a correction, and the right to see who has used the record and to whom it has been disclosed. Each of these elements is essential. The actual value of each of these rights depends on the current needs and interests of each data subject. Some people will go a lifetime without exercising any of these rights. Others will do so regularly. The need for accounting is fully justified by the privacy interests of data subjects.

For any covered entity, audit logs are also essential to protect the interests of the covered entity. It is apparent that health records are an attractive source of information beyond treatment or operational purposes. Some health workers will, if unimpeded, look up records of their coworkers, relatives, neighbors, celebrities, public figures, and others. Those who are overtly dishonest will sell patient information to crooks, fraudsters, and identity thieves. We have already seen these kinds of activities occurring; they have been well-documented in the press and in criminal cases. Audit logs for use and for disclosure are a principal way to enforce privacy rules within a covered entity and to deter misuse of records. The need for audit logs is fully justified by the institutional interests of covered entities.

Recording information about the use and disclosure of health records serves the interests of both record keepers and record subjects. Both have different needs, but much of the same information is need for both purposes.

However, there is one group of data subjects for which accounting records are crucial and, perhaps, even life saving. Those individuals who are the subject of medical identity theft (MIT) need to know how their records have been both used and disclosed in order to protect themselves from receiving inappropriate treatment or from being denied benefits because of the presence or disclosure of incorrect information resulting from the activities of the medical identity thief.

The World Privacy Forum does not believe that it is necessary at this late date to explain or detail for the Department the problems presented to patients and to covered entities by MIT. Our report on MIT – *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You* – remains a basic reference that is still current. See http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf. The title of the report underscores the crucial importance of correcting health records contaminated by information about a third party.

Associated with the report is a set of FAQs for victims of MIT that the WPF maintains on its website at http://www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html. Of the five sets of related questions, one entire set addresses how a MIT victim can and should use accounting records. The basic point as set out in FAQ 2 (Why should I care about accounting of disclosures?) is:

> If you think that you may be a victim of medical identity theft, obtaining a copy of the accounting of disclosures for your medical record will help you follow the trail of your information and identify those who have incorrect information about you.

Even if there were no other reason to keep accounting records, the needs of MIT victims would be sufficient alone to justify their maintenance. The problem of MIT will certainly grow worse as more health records become electronic and more interconnected. The WPF believes that, for electronic records certainly, accounting records should be maintained for all uses and all disclosures **without exception**. Nothing has happened in recent years to change that view.

5. With respect to treatment, payment, and health care operations disclosures, 45 CFR 170.210(e) currently provides the standard that an electronic health record system record the date, time, patient identification, user identification, and a description of the disclosure. In response to its interim final rule, the Office of the National Coordinator for Health Information Technology received comments on this standard and the corresponding certification criterion suggesting that the standard also include to whom a disclosure was made (i.e., recipient) and the reason or purpose for the disclosure. Should an accounting for treatment, payment, and health care operations disclosures include these or other elements and, if so, why? How important is it to individuals to know the specific purpose of a disclosure— i.e., would it be sufficient to describe the purpose generally (e.g., for ''for treatment,'' ''for payment,'' or ''for health care operations purposes''), or is more detail necessary for the accounting to be of value? To what extent are individuals familiar with the different activities that may constitute ''health care operations?'' On what do you base this assessment?

Response: The definition of the HIPAA term *health care operations* has about 400 words. That's more than a page of text. Even then, the definition is not complete as it uses the term *including* or *including but not limited to* several times. Most doctors would not understand the term. Most individuals would not understand the concept or many of its components. Telling an individual that his/her record was used for *health care operations* will convey no meaningful information. An accounting must be much more specific and must tell individuals about record usage and disclosure in terms that an average person can understand. Only a high-level health care executive is likely to fully understand the range of activities covered by *health care operations*.

The problem of providing information that individuals can understand goes beyond health care operations. It is challenging for any data subject who is not a well-informed health care insider to read and understand an accounting record. For any patient encounter – and especially for any in-patient stay – there can be dozens or even hundreds of individuals who will see the patient's record. The more information provided to the patient, the easier it will be for the patient to interpret the record.

This means that an accounting for TPO activities should identify the purpose in greater detail. A patient who learns that a treatment use or disclosure resulted in sharing of the patient's record with John Smith for "treatment" will learn nothing. If the accounting record states that John Smith was an x-ray technician, the activity is much more likely to be understandable. Just as important, an accounting record that has more detail will be less likely to result in additional questions (and additional expense) to the covered entity. Again, all interests are served by the recording of more detailed information about any use or disclosure, and by the release of that information to patients.

7. The HITECH Act provides that a covered entity that has acquired an electronic health record after January 1, 2009 must comply with the new accounting requirement beginning January 1, 2011 (or anytime after that date when it acquires an electronic health record), unless we extend this compliance deadline to no later than 2013. Will covered entities be

able to begin accounting for disclosures through an electronic health record to carry out treatment, payment, and health care operations by January 1, 2011? If not, how much time would it take vendors of electronic health record systems to design and implement such a feature? Once such a feature is available, how much time would it take for a covered entity to install an updated electronic health record system with this feature?

Response: The WPF strongly supports the accounting provisions. We do understand that accounting has costs, and the costs must be considered when designing the proper policy. A new accounting requirement for an old system can be particularly expensive to implement. One way to reduce the cost of new accounting requirements is to make them prospective only so that the requirements apply only to new computer systems (or systems with major software revisions) placed in service in the future. We support allowing a reasonable delay of implementation until installation of the next new computer change allows for meeting additional accounting requirements without special effort or for a limited period of years, whichever comes first.

***

We have several additional points to raise with respect to accounting.

A. An individual who has a right to an accounting record should be able to access the record online. As patients become used to online access to health records, accounting records should keep pace. If accounting records were available online, their use would increase. Patients today do not ask for accounting records because it is difficult or because they do not know about their rights. Online access would make a big difference. We suggest that a requirement for online access be implemented on a schedule that takes into consideration the current capabilities of computer systems maintained by covered entities. HHS should require online access to accounting records with a reasonable lead-time and in parallel with other activities that increase patient access to online health records.

B. The rule and the HITECH Act include time limits on a patient's right to access accounting records. Some limits may be appropriate, but it will often be the case that a covered entity maintains accounting records for a longer period than is required by the rule or the Act. Many will keep accounting records indefinitely. We believe that the proper policy would allow a patient access to any accounting records maintained and readily accessible by a covered entity without time limit. Thus, if a hospital's computer system maintains accounting records for 25 years, the patient should be able to access all of those records. The basic rule should be a simple one**: If a covered entity can access accounting records, then the patient should be able to access those records too**. We are not proposing a specific standard for the maintenance of accounting records, but if the records are kept, then patients should be able to obtain the records. If a covered entity discards accounting records but maintain audit logs, then the audit logs should be available to patients.

C. The benefits of accounting records and audit logs as both oversight mechanisms and deterrents against misuse of health records will not be realized unless the covered entity maintaining the records uses them in a constructive way. That should be a specific requirement that each covered entity review its accounting records (or audit logs) on a regular

basis, whether through automated means or otherwise. The existing HIPAA sanctions policy should lead to actions against employees who are abusing their privileges.

D. The current rule does not require a covered entity to maintain an accounting record for a disclosure made with the written consent of the data subject. This is an especially poor policy choice, and it will grow worse in the coming electronic environment. Patients are likely to be asked to give consent more frequently when records are electronic. Patients who opt into a Health Information Exchange could find all the disclosures to the HIE "exempted" from accounting because of the consent. That is not a good result. In fact, it would be a terrible and perhaps deadly result for MIT victims.

We note as well that the HITECH Act makes is much more difficult for a covered entity to refuse to make a consensual disclosure. The policy of the Act makes much sense if a patient wants another doctor or a lawyer to review the patient's records. However, the policy makes little sense if a marketer has wheedled consent ("Sign here for a chance to win a free t-shirt!") from a patient, something we fear may happen more frequently when records are electronic. Patients who have unwisely signed a consent form giving a third party full access to their records are not likely to remember or to realize that they have done so.

Unless the covered entity maintains accounting records for consensual disclosures, a patient may have no effective way to find out about the consent and to take action to stop future disclosures. Accounting records may be the only way to give a patient a fighting chance to protect his or her interests. Any covered entity is certain to keep a record of a consensual disclosure, just to protect its own interests. Make sure that the patient has the right to receive information about a consensual disclosure so that the patient can correct a mistake made in the past or stop disclosures that no longer serve the patient's interest. It would be egregious if a covered entity were routinely making consensual disclosures about a patient but the patient had no ability to learn about the disclosures.

Thank you for the opportunity to comment. If there are any questions or follow up, please contact us.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org
760-268-0094