WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

To the US Department of Health and Human Services

On the Proposed Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act (RIN 0991-AB57)

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

September 13, 2010

The World Privacy Forum appreciates the opportunity to submit comments on the Department's proposed changes to the HIPAA Privacy Rule, RIN 0991-AB57. The proposed rule appeared in the Federal Register on July 14, 2010, at 75 Federal Register 40868, <http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf>. The World Privacy Forum is a non-profit, non-partisan public interest research group, with a focus on research and analysis of privacy issues, along with consumer education.[1]

We have comments on several aspects of the Department's proposed changes to HIPAA. Of most concern to us are the proposed changes regarding marketing, among others.

1. Personal Health Records

> III. Section-by-Section Description of the Proposed Amendments to Subparts A and B of Part 160
>
> C. Subpart A—General Provisions, Section 160.103—Definitions.
>
> 2. Definition of "Business Associate"
>
> b. Inclusion of Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as well as Vendors of Personal Health Records

[1] For more information, see <http://www.worldprivacyforum.org>.

The NPRM appropriately provides that a business associate includes "a person who offers a personal health record to one or more individuals on behalf of a covered entity." This is what the HITECH Act provides.

The phrase *on behalf of* is already used in the definition of *business associate*, and it works well in that context. But a PHR is a more complicated animal. The HITECH Act definition is:

> (11) PERSONAL HEALTH RECORD.--The term ``personal health record'' means an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

We see the potential for confusion and manipulation here. A PHR vendor is a business associate if it offers a PHR to individuals *on behalf of* a covered entity. But a PHR is *managed, shared, and controlled by or primarily for the individual*. The PHR vendor potentially serves two masters here, and that is the source of the problem. For most covered entity functions, the *on behalf of* standard works well because the covered entity is the person who controls the relationship. That is not so clear with a PHR managed, shared, and controlled primarily for the individual. It is certainly likely to be true that these distinctions will not be understood by most consumers.

We are also concerned that the loose *on behalf of* standard can be easily manipulated by a covered entity and PHR vendor in order to evade coverage under HIPAA. Consider two nearly identical arrangements. In the first, the covered entity and PHR vendor agree that PHRs are offered to patients on behalf of the covered entity. That vendor is clearly a covered entity. In the second arrangement, the covered entity and PHR vendor have the same contract, except that it states that PHRs are offered *on behalf of* the individual or on behalf of the vendor. The vendor is, at least arguably, not a covered entity.

The concern here is that form and not substance may be controlling. Covered entities and PHR vendors could manipulate HIPAA coverage through weasel words in contracts. We suggest that a few sentences from HHS are needed here to clarify the potential relationships between covered entities and PHR vendors. **HHS should state that if there is any substantive contractual or other significant relationship between entity and vendor with respect to the provision of PHRs to individuals, then the PHR vendor is a business associate**.

We have a similar concern with respect to the meaning of *managed, shared, and controlled by or primarily for the individual*. A PHR vendor can define the purposes of a PHR simply by stating another purpose and giving it equal weight to the purpose of serving the individual. A website that maintains health information on individuals in connection with a covered entity might seek to evade the definition by stating that the records will also be used for a research purpose as well as being used by the individual. With two purposes, then arguably neither may be a primary purpose. Additional purposes can be invented as needed to evade the *primarily* test.

We understand the need to avoid covering records maintained primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business

purposes. However, *primarily* is a weasel word, and some will manipulate it to evade coverage by HIPAA. We think that HHS should explain that if records are made available for regular use or review by the individual, then that activity meets the test of *being managed, shared, and controlled by or primarily for the individual*, regardless of any other stated uses.

We reiterate that at the care level, when a patient is reading a privacy policy, the terms *on behalf of*, and so forth in a privacy policy will be unclear at best. In the area of sensitive patient information, patients deserve and should have complete clarity as to these business relationships and whether or not their PHRs are covered under HIPAA or not.

2. Marketing

> VI. Section-by-Section Description of the Proposed Amendments to the Privacy Rule
>
> B. Section 164.501—Definitions.
>
> 2. Definition of "Marketing"

The Department proposes changes in the rules about marketing that, in our opinion, are contrary to the law and the intent of the HITECH Act. We have no doubt that the language and intent of the HITECH Act restrict marketing activities, with the exception of prescription reminder letters, which are specifically authorized. Congress's goal was to limit marketing. It did so in several ways.

First, it prohibited a covered entity from "directly or indirectly receiv[ing] remuneration in exchange for any protected health information." [HITECH Act, 13405(d)]. That is a broad provision, whose purpose was to ban marketing activities flatly. The word *indirect* indicates a sweeping intent. The law prohibits a covered entity from receiving a payment or benefit of any type from any third party for a use that involves protected health information (PHI) by the covered entity. We think this provision even prevents a covered entity from showing patients advertising that encourages the purchase or use of a good or service. That's how broad the statutory language is.

Second, Congress closed the loophole that allowed some marketing activities to be conducted as health care operations. Section 13406(a)(2) says expressly that a covered entity cannot engage in any marketing activity under the guise of a health care operation if the entity receives a direct or indirect payment. Again, we find the same broad *direct or indirect* language. The intent to restrict marketing using PHI is clear.

The exception in the statute demonstrates the sweeping scope of the policy. The statute allows a reminder letter for a drug already being prescribed. However, a letter seeking to switch a patient to another drug is effectively prohibited by this provision, which excludes all other marketing. The conference report makes the purpose quite clear: "The conference report makes an exception and allows providers to be paid reasonable fees as determined by the Secretary to make a communication to their patients about a drug or biologic *that the patient is currently prescribed*." By specifying that this type of marketing activity is allowed, Congress made it clear

that all other marketing activities (other than the few activities allowed by the rule already) are prohibited without express patient authorization.

Third, in § 13405, Congress prohibited the sale of any PHI without an authorization. There are some exceptions in § 13405 that are not relevant to marketing. This provision is further evidence that Congress does not want patient records to be made available for marketing activities. Congressional opposition to marketing activities is quite clear. Our principal concern here is that those seeking to market to patients will use every means to exploit every loophole to conduct marketing. If a third party can find a way to pay a covered entity to send a health-related communications to an individual about the third party's products or services, that third party will do so. The enormous sums (measured in the billions) spent on direct-to-consumer drug advertising are evidence of the stakes here. These sums are spent to urge patients to seek high-priced, patent-protected drugs that reap enormous revenues for drug manufacturers. There is no evidence that this advertising produces better outcomes or lower costs. Indeed, this advertising will only continue as long as the revenues that result from advertising exceed the cost of the advertising. Patient outcomes and overall health care costs are not factors in marketing decisions.

We agree with the statement in the NPRM that:

> Congress intended with these provisions to curtail a covered entity's ability to use the exceptions to the definition of "marketing" in the Privacy Rule to send communications to the individual that were motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication's being about a health-related product or service." 75 FR 40884.

In our view, the new law requires that paid communications for any marketing should be allowed only on an opt-in basis. <u>We oppose in the strongest possible terms the proposal that would allow communications paid for by third parties who are not the entities whose product or service is being described in the communication</u>. The Department's description is:

> We also emphasize that financial remuneration for purposes of the definition of "marketing" must be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described. For example, authorization would be required prior to a covered entity making a communication to its patients regarding the acquisition of new state of the art medical equipment if the equipment manufacturer paid the covered entity to send the communication to its patients. In contrast, an authorization would not be required if a local charitable organization, such as a breast cancer foundation, funded the covered entity's mailing to patients about the availability of new state of the art medical equipment, such as mammography screening equipment, since the covered entity would not be receiving remuneration by or on behalf of the entity whose product or service was being described. Furthermore, it would not constitute marketing and no authorization would be required if a hospital sent flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party, since the financial remuneration to

> the hospital from the third party was not in exchange for the mailing of the flyers. 75 FR 40885.

If the Department allows third parties to fund marketing communications, the result will be the laundering of marketing funds through non-profit organizations established by drug and device manufacturers to promote high-priced, patent-protected drugs and devices. It is child's play for a large, wealthy drug manufacturer to establish and fund an independent non-profit whose principal function will be to fund advertising that the manufacturer cannot directly pay for itself. Many hospitals, especially those that are not-for-profit, have associated foundations that could provide the necessary "cover".

The Department's proposal would allow indirectly precisely what the law and the other parts of the proposed regulation seek to prohibit directly. Even worse, manufacturers who utilize non-profits to hide their advertising dollars will be able to take a charitable tax deduction for the contributions given to the non-profits that are to be used to fund the marketing activity. Manufacturers may also utilize existing non-profits, who may welcome a few dollars in exchange for laundering marketing to patients. Money talks, and financially strapped non-profits may, unfortunately, listen to the money more than they should.

From the perspective of the patient whose data is being employed in the marketing activity, the source of funds for the communication makes no difference. Patients receiving marketing communications will see only that their PHI has been used and that their confidentiality has been breached. It will not matter one iota that the communication was paid by a non-profit. The message to patients will be that patient records are now available for any and all marketing uses, and that patients should be wary about revealing their personal information to health care providers lest it be used for marketing. Labeling the communications will not help. Patients will not see or appreciate what the labels tell them. The rules as proposed would confuse lawyers, let alone the average person with a 9th grade reading level. You cannot cure a bad policy with a label.

The proposed regulations contain another troubling point. The Department would allow providers to be paid by third parties to engage in marketing paid for by third-parties in the guise of treatment communications:

> [W]e do not propose to require individual authorization where financial remuneration is received by the provider from a third party in exchange for sending the individual treatment communications about health-related products or services. However, to ensure the individual is aware that he or she may receive subsidized treatment communications from his or her provider and has the opportunity to elect not to receive them, we propose to require a statement in the notice of privacy practices when a provider intends to send such subsidized treatment communications to an individual, as well as the opportunity for the individual to opt out of receiving such communications. 75 FR 40886

We recognize that Congress expressly addressed marketing in the context of health care operations. It did not expressly ban paid marketing by providers under the guise of treatment.

However, the congressional intent is clear. Marketing is an unfavored activity in this context, and the only paid marketing allowed is for prescription reminders. Why would Congress have been so specific in this area if marketing activities could be conducted with as few limitations as treatment? We submit that any doubts, any ambiguity must be resolved in favor of the policy that Congress expressed in the HITECH Act. Whether a marketing activity is treatment or a health care operation, it should be as severely restricted as possible.

To allow third-party funded advertising with an opt-out ignores the widespread rejection of opt-outs in privacy discussions taking place elsewhere. Regulators elsewhere in government are looking for alternatives to opt-out as a privacy protection. Legislators are considering proposals that might allow opt-out in some circumstances, but would generally require *opt-in* (affirmative consent) for health and other sensitive information. History shows that opt-outs are rarely utilized by individuals because they are hidden, cumbersome to use, or ignored. There is little evidence that people read notices of privacy practices (NPP) that they receive. Essentially, the current HIPAA rule regarding NPPs as implemented by many covered entities has already taught people that the NPPs are not important or worth reading. Placing a notice of opt-out in an NPP or similar document will not inform patients of their opt-out rights in any meaningful way.

The only entities today that support opt-out are those who benefit from the inability of individuals to opt-out. The more opt-outs available to individuals, the less likely it is that individuals will use them. The burden of opting out at every website, every merchant, every health care provider is and will be overwhelming. The likelihood of successfully protecting personal information through opt-out will be perceived by many individuals as low. Whatever the Department's position on the value of opt-out generally as a privacy protection device, it is imperative that any doubts be resolved against the use of opt-outs for sensitive information contained in health records.
Further, polls suggest that most patients want to exercise personal control over the use of their information for research and to be asked for permission for their records to be made available to researchers. It is not hard to extrapolate that even more would want to have the ability to exercise affirmative consent prior to the use of their information for marketing. Therefore, the simplest rule – the least expensive to administer – is one that makes the default what people want, which is no use of PHI for marketing.

We remind the Department that there are many providers who have information on each patient. A patient's information may be held by or accessible to a hospital, physician, laboratory, x-ray facility, pharmacy, and many more providers. A patient may have no direct relationship with some providers and have no idea why, for example, a laboratory that the patient never heard of is profiting by using the patient's information to send advertising to the patient based on a test result.

Each provider with access to patient information may be in a position to send advertising on behalf of third parties. A family of four may have to take separate action on behalf of each family member to opt-out of communications by each physician, each laboratory, each pharmacy, each x-ray facility, and more. That family might be obliged to opt-out dozens of times. No matter how easy it may be to opt-out in one given instance, the total burden will be

overwhelming. If a patient opts-out of receiving paid advertising by one provider, the next provider can still send the same ad. Opt-out again, and a third provider can send the next ad. Then a fourth provider, and so on. There is no simple, quick, and inexpensive way to opt out if you have to opt out over and over again.

Faced with the effective impossibility of opting-out and having it stick, even the rational patient who strongly opposes use of his or her information for marketing will give up, defeated by a lax Department policy that favors marketing over privacy and that does not give patients any real chance of protecting their own health privacy. There is no way to structure an opt out that will give a patient an even break.

We also remind the Department that efforts to make health records electronic may place patient information in the hands of more and more health care providers than ever before. This will only increase the marketing possibilities and will further overwhelm patients who seek to exercise any rights that they may have. As patient health care activities migrate to the Internet, the advertising that the Department proposes to allow without patient authorization will also migrate to the Internet. Patients who click casually on ads may not realize that the ad was served only to patients with a particular disease, with a certain net worth, who own their homes, who have a health care plan that covers high priced drugs, who have children, etc. The ad will not reveal how patients were selected to receive it.

No matter what disclosures are made, the patient who clicks an ad may be sharing personal information – health related or otherwise – with an advertiser who is then free to use the information without any legal or regulatory restriction. Patient privacy may well be fatally undermined as a result, as patient information leaks over time into the unregulated files of marketers and profilers, who will then profit from its use and sale indefinitely. For genetic information, PHI may retain marketing value for generations.
Further, allowing physicians and other health care providers to profit by receiving remuneration for recommending specific types of treatment should be illegal and is certainly unethical. Why the Department wants to support this conduct is a mystery. The Department has enough difficulty already controlling self-dealing by providers. Giving providers another way to profit by taking money to promote products and services is unsupportable.

We suggest that any controls on the amount of financial remuneration will be unenforced and ineffective. The Department does not have enough resources to police HIPAA today. Overseeing and enforcing payment limitation will not be a priority. If anyone exceeds the vague limits proposed, they will happily pay a fine in the unlikely event that they are caught. We do not have to discuss the possibility of under-the-table or disguised payments that will be impossible to trace. The Department well knows that drug manufacturers are happy to pay physicians for "lectures" or other activities that are proxies for prescribing their medications.

In conclusion, we do not understand why the Department is showing any interest in allowing new marketing uses and disclosures without specific patient authorization. The Department offers no evidence that marketing using PHI improves outcomes or lowers costs. We believe that the contrary is true. Only high priced, patent-protected drugs and devices will be marketed, and the marketing will continue only as long as the manufacturer's profits increase and without

regard to better outcomes. From an advertiser's perspective, higher revenues and higher profits are the only important outcome. Allowing marketing will further undermine the Department's efforts to control health care costs.

If health plans controlled marketing uses of PHI, it is likely that they would not seek to promote expensive medications. Unfortunately, some in the health care system do not care what the costs are. Some pharmacies have demonstrated a willingness to send marketing materials to patients for the few cents that they earn from the communication and the additional prospect of an additional small profit from a prescription refill. These providers do not care what the costs are to other participants. The Department has to look at the issue with a broader perspective.

We suggest that the Department take with a grain of salt the pleas by marketers that giving patient additional information is valuable and educational. If a patient should receive additional information, why is that information only available in connection with the marketing of high-priced, patent protected drugs and devices? If there are benefits here, we think it would be less costly overall to require that information useful to patients be included with other disclosures that are already required. If the cost of conveying additional information is billions of dollars in extra profits to manufacturers, then the price is too high. We think that a cost benefit analysis is appropriate here. The Department should not pay attention to a cherry-picked analysis of the supposed value of the information to consumers.

We have an additional suggestion. It is our understanding that prescription reminder programs are often structured so that not all patients receiving the drug in question receive a reminder. Some patients are not sent reminders so that they serve as a "control". That allows the drug manufacturer paying for the reminder to tell if the reminders increase revenues. This practice is unfair and obnoxious. It is bad enough that patients only receive paid reminders for drugs that are highly profitable. Advertisers may also be discriminating against patients based on other characteristics, such as the type of health insurance they have. The Department should require those paying for refill reminders to send reminders to all patients, including those taking generics. If these programs are justified because there is a patient benefit, then all patients should receive the benefit.

The Department should change the rule to allow reminders only if they are sent to all patients and without regard to their incomes, the type of health plan, the nature of prescription drug coverage, or any other characteristic. A policy of non-discrimination is essential.

3. Business Associates

C. Business Associates.

1. Section 164.502 – Uses and Disclosures.

Proposed new provisions at § 164.502(a)(4) and (5) address the permitted and required uses and disclosures of PHI by business associates. Specifically, proposed § 164.502(a)(4) would allow business associates to use or disclose PHI only as permitted or required by their business associate contracts or other arrangements pursuant to § 164.504(e), or as required by law. If a covered entity and business associate have not entered into a business associate contract or other arrangement, then the business associate would only be allowed to use or disclose PHI *as*

necessary to perform its obligations for the covered entity (pursuant to whatever agreement sets the general terms for the relationship between the covered entity and business associate) or as required by law. 75 FR 40887.

We do not object to this policy. However, we think that the standard is not clear enough. If there is no contract, the *as necessary* standard is too vague to work. Consider a business associate that would normally disclose PHI to an auditor, computer service provider, or outside lawyer in connection with its corporate activities. Are those disclosures *necessary*? Does the standard mean that if the disclosure can be avoided under any circumstances, then the disclosure must be avoided? For example, would a business associate be obliged to hire an in-house lawyer instead of using outside counsel? One could pose many other questions of this type. We obviously do not want business associates using PHI for inappropriate purposes, but a standard that is too strict will only cause problems. The Department can save everyone much time and expense by explaining or adjusting the standard so that its limits are clearer and more realistic.

For other provisions having to do with contracts and agreements with business associates and subcontractors, the Department would be well advised to draft specific contracts or specific language for covered entities to use. Otherwise, each lawyer in each covered entity will draft language, and every version will have small and unnecessary differences. As the chain of data and contracts goes to three, four, or more levels of business associates and subcontractors, reconciling the differing language will take more and more expensive lawyers' time. We do not suggesting mandating the use of specific language, but the Department could save everyone considerable sums if it offered standard language and, at a minimum, urged covered entities and others to use the standard language in the absence of specific justification. No one benefits when lawyers duplicate efforts.

4. Sale of Protected Health Information

> D. Section 164.508—Uses and disclosures for which an authorization is required.
>
> 1. Sale of Protected Health Information

In 13405(d)(1), the HITECH Act provides that a valid authorization for sale of PHI must include "a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual."

> In response, the Department proposes:
>
> We do not include language in proposed § 164.508(a)(4) to require that the authorization under § 164.508 specify whether the protected health information disclosed by the covered entity for remuneration can be further exchanged for remuneration by the entity receiving the information. We believe the intent of this statutory language was to ensure that, as currently required by § 164.508 for marketing, the authorization include a statement as to whether remuneration will be received by the covered entity with respect to the disclosures subject to the authorization. Otherwise, the individual would not be put on notice that the disclosure involves remuneration and thus, would not be making an informed

> decision as to whether to sign the authorization. Accordingly, we propose to require that the § 164.508(a)(4)(i) authorization include a statement that the covered entity is receiving direct or indirect remuneration in exchange for the protected health information. This requirement would ensure that individuals could make informed decisions regarding whether to authorize disclosure of their protected health information when the disclosure will result in remuneration to the covered entity. We also note, with respect to the recipient of the information, if protected health information is disclosed for remuneration by a covered entity or business associate to another covered entity or business associate in compliance with the authorization requirements at proposed § 164.508(a)(4)(i), the recipient covered entity or business associate could not redisclose that protected health information in exchange for remuneration unless a valid authorization is obtained in accordance with proposed § 164.508(a)(4)(i) with respect to such redisclosure. We request comment on these provisions. 75 FR 40890.

We admit to being mystified that the Department has decided to ignore a direct statutory requirement. The explanation that a recipient covered entity needs its own authorization for a further disclosure is, if always true, something that the Congress already knew. Yet the Congress chose to add the requirement anyway. Recipients of PHI under an authorization may not always be covered entities or business associates covered by the rule. We would be happy to see all subsequent exchange for remuneration flatly banned, in which case the congressionally-mandated specification could be ignored as truly not necessary.

Additionally, in proposed § 164.508(a)(4)(ii)(C), the Department would create an exception from the authorization requirement for disclosures of PHI for treatment and payment purposes, in which the covered entity receives remuneration. We are concerned about the inclusion of payment information sales. Will these disclosures be to others who are not covered entities? If so, then the sale of PHI for payment could put the sold information entirely outside the HIPAA privacy rule. Researchers who buy PHI are not covered by the rule. Is this a possible result for purchasers of information for payment purposes?

We believe that the sale of receivables will result in information escaping from privacy coverage. If the Department allows the sale of receivables for a payment purpose, any recipient must remain bound by the rule just as any business associate would be. With the proper explanation, the proposed inclusion of payment sales is not objectionable. We note that allowable sales for health care operations must be to covered entities only.

5. Compound Authorizations for Research

> 2. Research.
>
> a. Compound Authorizations

The Department proposes to amend § 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research

components and clearly allows the individual the option to opt in to the unconditioned research activities.

The WPF does not think that this change is justified by any facts. The Department states:

> For clinical research trials that may have thousands of participants, documenting and storing twice as many authorizations is a major concern. There is also a concern that multiple forms may be confusing for research subjects. The Department has received reports that recruitment into clinical trials has been hampered, in part, because the multiplicity of forms for research studies dissuades individuals from participating in research. We have also heard that redundant information provided by two authorization forms (one for the clinical study and another for related research) diverts an individual's attention from other content that describes how and why the personal health information may be used. 75 FR 40893.

There may be a concern here, but we doubt strongly that it is a *major* concern. Combined forms may be just as confusing to subjects, if not more so. Does HHS know how many forms are currently used in research projects and whether one less privacy form would make be a significant reduction in the number of forms that patients fill out (especially if they participate in research activities involving treatment)? The existence of a "concern" without documentation of that concern is meaningless. Reports that the Department has received or heard are not justification for a change in the rule.

If any community is capable of providing hard evidence, it is the research community. Yet there is no evidence cited in the proposed rule. Complaints by lazy research administrators are not hard evidence. We have heard concerns from researchers that telling potential research subjects about their rights discourages them from participating. That is their real concern. Too many researchers are interested in recruiting participants and not in informing those participants of their rights. The Department has to stand up for research subjects or no one will. We do not think that the Department has justified the change in this rule and we urge the Department to omit this change.

6. Authorizing Future Research Use

b. Authorizing Future Research Use or Disclosure

The Department is considering whether to modify its interpretation that an authorization for the use or disclosure of PHI for research be research-study specific. We agree that there is somewhat more justification for looking at this requirement (as compared with the proposed change in compound authorizations). The propose rule sets out three ideas.

> In particular, the Department is considering a number of options and issues in this area, including whether: (1) the Privacy Rule should permit an authorization for uses and disclosures of protected health information for future research purposes to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her protected health

> information could be used or disclosed for such future research; (2) the Privacy Rule should permit an authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule, and if so, what should those be; and (3) the Privacy Rule should permit option (1) as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research.

We do not choose to support or oppose any of these options. Our view is that there must be a limit of some sort to these authorizations. They cannot be allowed to continue indefinitely. A 21-year-old research subject who casually signs an authorization that he did not fully understand at the time could remain a research subject for decades, without any further notice.

The recent widely reported incident involving the collection of blood samples for research from the Havasupai Indians is instructive here. While the reports suggest that the Indians signed a broad consent, when the Indians learned later of some of the uses, they were upset. They sued and ended up with a significant monetary settlement and return of their blood samples. See Amy Harmon, *Indian Tribe Wins Fight to Limit Research of Its DNA*, New York Times, April 21, 2010, available at <http://www.nytimes.com/2010/04/22/us/22dna.html>. Broadly written, long-lasting authorizations will only lead to more litigation and more expense. If researchers are left as gatekeepers for research uses of PHI, the researchers will act in their own interest and not in the patients' interest.

In addition, those who have signed more open-ended authorizations will find it difficult at best and impossible at worst to find the researcher to revoke the authorization. Further, if a researcher or research institution can pass a project (and the authorizations associated with it) to another researcher, it would be impossible for most research subjects to discover what happened to their data.

Another undesirable consequence of extending authorizations indefinitely would be to deny research subjects access to their data when the project is over. As the rule stands today, a research subject receiving treatment may be unfairly and indefinitely denied access to essential information about his or her treatment during the course of a research trial. This denial of rights will only get worse if projects extend into other projects indefinitely. We do not have a specific proposal other than to ask that there be some firm ending to authorizations that continue in effect beyond the specific project for which they were obtained. We agree that some will perceive that genetic analyses are sensitive, but so are many other medical activities. It is hard to distinguish between sensitive and non-sensitive health information.

Just to pick one example, we rather doubt that anyone above the age of five would consider bed-wetting to be a non-sensitive health issue. If no other limit can be found, we suggest that the Department impose a term of years on an authorization for research purposes not related to the specific purpose for which the authorization was obtained. We suggest a limit of two years.

7. Decedent Information

E. Protected Health Information About Decedents.

1. Section 164.502(f) -- Period of Protection for Decedent Information.

We support the Department's proposal to limit the scope of HIPAA so that it does not cover persons who have been deceased for more than 50 years. Any term of years is necessarily arbitrary, and 50 years is one of several reasonable periods that could have been selected and that we might have supported as well. However, we believe that HHS should explain that the termination of HIPAA obligations does not change any other requirement that may be imposed on a covered entity by state law, by other federal laws, by contractual obligations, or by professional ethics.

HHS should make it clear that it is up to a covered entity to determine what to do with a health record at the 50 year mark and that the termination of HIPAA coverage does not make the record public. While most records of long-dead individuals will have no public interest, some may. We note that an x-ray of Marilyn Monroe recently sold at auction for $45,000. See <http://www.nydailynews.com/money/2010/06/28/2010-06-28_marilyn_monroes_chest_xray_from_1954_sells_for_45000_at_las_vegas_auction.html?r=entertainment>. We think it would be unfortunate if a covered entity chose to sell celebrity health records at the 50 year mark, and HHS should at the very least discourage this type of conduct even if it no longer regulates it.

8. Student Immunizations

F. Section 164.512(b) -- Disclosure of Student Immunizations to Schools.

We have no comment on the disclosure of immunization information based on an oral authorization, except to suggest that any change make it clear that covered entities must comply with the requirement for an accounting of the disclosure. The rule already and unwisely exempts disclosures based on authorization from the accounting requirement. We would be happy if the Department chose to revisit that exemption.

In this case, however, an oral authorization must have an accounting of the disclosure because no other documentation will exist. There will be no written authorization that a patient might be able to obtain or discover. There must be some accountability here and the ability for tracking.

9. Fundraising

H. Section 164.514(f) -- Fundraising.

The Department requested comment about what fundraising communications the statutorily required opt-out should apply. The answer is very simple. **Once a patient opts out, the opt out should cover all future fundraising communications, except where a patient has expressed a willingness to receive future communications.** Asking a patient to opt-out of each particular fundraising campaign would only invite abuse. Any expressed opt-out must be permanent and

comprehensive. Opt outs are already stacked against the interests of data subjects. Requiring repeated opt outs for the same activity would only make it worse and would invite abuse. A hospital could simply define each month's fundraising activity as a separate campaign to evade an opt out. We see nothing in the statute that suggests or allows a fundraising opt-out to be anything other than permanent with respect to a covered entity.

The Department also seeks comment regarding the prohibition on use or disclosure of certain treatment information without an authorization. Sharing any health information with a fundraiser is a gross violation of privacy. Telling a fundraiser that the patient was treated by a particular department can be tantamount to disclosing the diagnosis. Sharing outcomes information is just as bad. Consider a person who had told no friend or family of her cancer treatment who subsequently receives a call from a stranger who knows about that treatment. How can any such use be justified under any circumstances? The NCVHS recommendation is simply wrong here. Imagine that a hospital hired a business associate to do fundraising and that you received a call from a neighbor, cousin, or colleague working for that fundraiser who knew that you were treated by the oncology department?

If a hospital wants to avoid soliciting patients with bad outcomes, it can do so by only giving its fundraisers information about patients with good outcomes. That can be done internally, using health care providers or computers to make the judgment and without sharing any substantive health information with non-treatment personnel. We would not object to a change in the rule that allowed that particular narrow use as an exception.

10. Notice of Privacy Practices

> I. Section 164.520—Notice of privacy practices for protected health information.

We have little to say about the proposed changes to the NPP. However, we take exception to one statement in the explanation.

> The proposed provision would ensure that covered entities provide notice to individuals indicating that most disclosures of protected health information for which the covered entity receives remuneration would require the authorization of the individual.

The proposed marketing rule would, in fact, allow virtually unlimited remuneration uses and disclosures of one type or another without authorization. We propose that all of these uses and disclosures be prohibited. However, it is disingenuous for the Department to suggest here that *most* marketing disclosures will require patient approval. The other changes to the notice about marketing do nothing to allay our substantive concerns about marketing uses. Regardless, as we suggest above, few patients will read or understand the notices.

11. Right to restrict

> J. Section 164.522(a)—Right to request restriction of uses and disclosures.

The Department has done a good job in the proposal of setting out the problems and potential conflicts that the new right to restrict presents. We do not have comments on many of the specific issues raised. Generally, we think that the rule must make it clear that a health care provider must allow a patient to pay out of pocket rather than rely on insurance. We are concerned that providers may want to avoid the headache and additional expense that the right to restrict entails.

Otherwise, we have a general suggestion. We believe that the right to restrict provision should not be implemented with a detailed set of rules governing all the possible problems that are identified in the proposal. No matter how many circumstances are covered by rules, other unanticipated circumstances will arise that were not foreseen. While there may be a need for details in some circumstances, we think that the Department would do better instructing health care providers to implement the requirement *in good faith and in consultation with the patient whenever conflicts, problems, or questions arise with respect to a specific request*. The Department might supplement a "good faith" obligation with FAQs that give examples of how specific problems might be addressed in practice.

We have learned from the detailed HIPAA privacy rule that the more the Department says about implementation of a specific requirement, the more confusion results. Lawyers keep presenting hard questions, and when HHS tries to answer them, the results only breed more questions. It is too late to fix existing problems in this regard, but the new right to request a restriction is a good place to take a new tack. Mandating that providers implement this requirement in good faith and in consultation with the patient is a reasonable standard and more likely to achieve a good outcome than pages full of rules.

We observe as well that the statutory right to restrict use and disclosure will oblige the health care system to find a way to segregate some PHI from other PHI. Given the coming EHR environment, the WPF believes that there will surely be a need to segregate other types of health information in a health record in order to limit its use or disclosure, or to accomplish other purposes. The Department should use the opportunity presented by this rulemaking to learn how record segregation can be accomplished. The lessons learned here can instruct further EHR planning.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum
www.worldprivacyforum.org
760-436-2489