WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

To The Department of Health and Human Services

Regarding RIN 0991-AB62, Proposed changes to the HIPAA Privacy Rule regarding Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act

Via Regulations.gov

Office for Civil Rights
Attention: HIPAA Privacy Rule Accounting of Disclosures
Hubert H. Humphrey Building
Room 509 F
200 Independence Avenue, SW
Washington DC 20201

August 1, 2011

> **Re: RIN 0991-AB62, Proposed changes to the HIPAA Privacy Rule regarding Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act**

The World Privacy Forum appreciates the opportunity to submit comments on the Department's proposed changes to the HIPAA Privacy Rule regarding Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act. The proposed rule appeared in the Federal on May 31, 2011 at 76 Federal Register 31426, http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf.

The World Privacy Forum is a nonprofit, non-partisan public interest research group, with a focus on research and analysis of privacy issues, along with consumer education. WFP published *A Patient's Guide to HIPAA*, one of the few detailed, patient-focused guides to the law. The HIPAA guide receives heavy use on our website, http://www.worldprivacyforum.org/hipaa/index.html. For other WPF activities on health and other matters, see generally http://www.worldprivacyforum.org.

I. General Comments about NPRM

The World Privacy Forum supports some of the proposed changes, but we also want to see some significant revisions in the new accounting rule.

One overall troubling aspect of the NPRM is the Department's limited view. In some places, the Department recognizes the revolution in health care information that it is directing, and it expressly shifts the balance in its current accounting proposal to protect that future. However, the Department does not sufficiently take into account the changes that are coming for patients' use of their own health records.

In activities and pronouncements elsewhere, the Department foresees and promotes a larger role for patients in managing their own health care and health care information, for example, the Department has actively promoted electronic Personal Health Records as a consumer empowerment tool. In this NPRM, the Department too readily dismisses patient use of accounting records on the grounds that patients do not care and rarely use them. The Department's inconsistent view here is troubling.

A broader look at the exercise of HIPAA rights by patients also finds that patients today only occasionally exercise their broader rights to access health records. The Department and many others expect that to change. Patients will benefit from the revolution in health care information technology, and there is a reasonable chance that they may well utilize EHRs and PHRs. Greater patient use of their own health records is important to the analysis here. A patient who directs the sharing of his or her health information into a PHR can acquire, manage, and understand accounting information too. If the HIPAA rule gives patients a greater ability to monitor how their information is used and disclosed, patients will pay attention. Entrepreneurs, PHR vendors, patient rights organizations, and others will develop tools, including cell phone apps, to help patients learn what is happening to their records. We predict that these tools will cover accounting records and increase demand for and use of the records. We note that ***requests for accounting records are likely to be as routine as requests for substantive health records.***

It is a mistake to extrapolate solely from the existing accounting environment, where it remains difficult for patients to exercise their current rights, manage their own records, and understand the incomplete records that are available now as accounting records. Accounting records available to patients today are not likely to be useful to many patients. That will change with the new requirements.

Further, the Department and others have not done a good job educating patients about HIPAA rights. Partly as a result, patients have not exercised their rights extensively. The Department now extrapolates from current failures and assumes that the future will be just like the past, notwithstanding the massive change in health care information technology that is happening. We suggest that the right policy here is simple. ***Build the facility and educate patients, and more patients will use the records.*** That policy applies to accounting records as well as substantive patient records. A rising electronic tide will raise all boats.

We also suggest that the Department is not giving sufficient weight to the congressional judgment that more accounting for electronic records is a worthy objective. The facts of patient usage of accounting were known to the Congress, but it nevertheless expanded patient rights to accounting records because it had a vision of the future that included a greater role for patients, more robust patient privacy rights, and a greater need for accountability in an increasingly

electronic information environment. The Department needs to embrace the congressional action and carry out the intent to a greater extent than it has.

We observe that security breaches are a feature of today's record keeping activities. We see no reason why this will change in the near future. When a breach occurs, accounting records may be essential to determine responsibility. Without accounting records, covered entities who shared records with others may encounter litigation to determine who will pay the costs. A few lawsuits will cost more than any potential savings from shortchanging accounting records in the Rule.

Nevertheless, the World Privacy Forum recognizes that there are costs to accounting for access and disclosure, and that the privacy budget is never unlimited. There must be tradeoffs that include the cost of providing new or additional services. We recognize that more of everything is either not attainable, or is not attainable today.

One way to deal with the cost of new requirements is through the calendar. The Department needs to adopt a much longer-term perspective on accounting rules. If the Department sets the accounting bar too low today, then its choices will foreclose useful options and innovations that may be too expensive for a legacy system, but that will be inexpensive in a new system. Information systems will be designed to meet requirements, and it will be too expensive and politically impossible to change those requirements in the future once we have proceeded farther down the road. We reiterate: ***if the Department limits its rule to what is attainable at present, it will make records of access and disclosure unavailable in the future, when the maintenance and sharing of the records will be easier and less expensive.***

We believe that a better approach is to recognize current cost considerations and transitional problems by providing covered entities with a long lead time for some requirements.

We would rather see a broader and more useful accounting requirement included, even if it does not take effect for a decade rather than pass up the chance to include a valuable feature in the health information system of tomorrow. With enough advance notice, software and system developers can add required tools to new systems that will be much less expensive than retrofits of old systems. Storage costs will continue to drop as well. We are at a key junction right now, and the attention needed to provide better privacy facilities for future generations depends on the choices made today. The Department must anticipate the future and the availability of greater patient interest and better information tools. Patients will use accounting records when those tools exist. Costs will be lower with advance planning and broader mandates.

A note on language. In these comments, we use the term *patient* to refer to the subject of Protected Health Information (PHI) under the HIPAA privacy rule. We are aware that the rule uses the term *individual* – and that is precisely what we mean by *patient* – but we find the regulatory language more awkward to use in general discussion.

II. Specific comments

A. Two Separate Proposed Rights Can Be Stated As a Single High-Level Principle

On page 31428, the NPRM states:

> We are proposing to revise § 164.528 of the Privacy Rule by dividing it into two separate rights for individuals: paragraph (a) would set forth an individual's right to an accounting of disclosures and paragraph (b) would set forth an individual's right to an access report (which would include electronic access by both workforce members and persons outside the covered entity).

We support strongly the new proposed patient right, but we are troubled by the choices the Department made in how it has added the new patient right. This comment addresses only how the right is presented and not its substance. Again, we support the new right. We would like to see changes in its presentation.

It is hard enough to teach patients what their rights are. Adding a new right that is similar to an existing right is more likely to confuse than to clarify. The rule is already troubled by the use of the non-transparent term *accounting*, and the addition of a second non-transparent term *access report* will not help. This may be the last chance that the Department has to drop the word *accounting* altogether and replace it with a much clearer phrase, such as *use and disclosure history*. We suggest that the Department make the change in terminology now. Beyond terminology, the distinction between use and disclosure is not a simple one for consumers to grasp, and the application of that distinction in the health care setting is especially confusing because the same activity can result in a use or a disclosure for reasons that have nothing to do with the nature of the activity.

We suggest that the Department reconsider the bifurcation of the right to an accounting in two parts and that the broad right be stated as a single principle. The differences between the rights to accounting and to access reports should come at a secondary level. The high-level principle should be clearer, we suggest: ***Each patient has the right to know who has used his or her record and when and why the record was disclosed.***

B. Strong Support of Uses Provisions

The Department proposes to expand upon the provision in § 13405(c) of the HITECH Act by requiring information about uses as well as disclosures from an EHR. We strongly support this change. In making this choice, we applaud the Department for taking a forward-looking view of the developing health information infrastructure in this instance.

First, the information is essential to individuals who want to know how their records were used. Second, the distinction between use and disclosure is becoming increasingly artificial anyway. Third, the requirement builds on technology already in use to give patients better privacy rights without imposing new costs. If necessary, we would support a delay in this requirement if some covered entities need more time to comply with the provision in the security rule that is the

linchpin of the use accounting records. We would rather see an extended delay (years, if necessary) rather than passing up the opportunity to do the right thing.

We note that this step on accounting for uses is a forward-looking vision. We applaud this. It is not replicated in other parts of the NPRM, though. We again take the opportunity to say that the proposed new exceptions and limitations on accounting take a crabbed view, seeking to stop accounting for reasons that make little immediate sense and even less in the long run. We think that the Department needs to be as forward looking elsewhere in the NPRM as it is on accounting for uses.

C. Problematic Purpose of Access Language

On page 31438-39, the NPRM states:

> We are not proposing to require that access reports include a description of the purpose of the access. In response to our RFI, a majority of commenters indicated that we should not require that an accounting of disclosures for treatment, payment, and health care operations include the purpose of the disclosure. Commenters stated that this information is not currently captured when protected health information is accessed, and requiring the information would represent a significant disruption of workflow. The majority of commenters also indicated that individuals did not have a good understanding of terms such as "health care operations."

We believe that this it is a poor choice to deny patient information about the purpose of access.

First, we agree that patients do not understand the term *health care operations*. However, to conclude that no information is better than an unclear term is the wrong conclusion. The right conclusion is to provide other information that would be more meaningful. We believe that providing a statement of the purpose of a use is important to make the records meaningful to patients.

Second, we have strong doubts about the statement from "commenters" that purpose information is not captured. It is our understanding that at least some electronic health record systems already require uses to state the purpose of their access. We believe that the Department needs to look beyond statements that may be financially motivated and find more neutral facts here. Further, we believe that collecting an indication of the purpose of an access is likely to be commonplace in future computer systems, if only to allow covered entities to oversee and hold accountable their own employees.

We would accept a policy that limits the collection of purpose information to that which can be readily obtained electronically. It would be fine to ask a user to make a click and not write an essay to obtain access to PHI.

Third, the contrast between the information that patients receive about accesses and about disclosures will be noticed by patients. Patients will ask why they were told why a particular

disclosure was made when the same information is absent from the list of uses. Patients will figure out that some activities that are disclosures are essentially identical in purpose to activities that are uses, and they will be curious or suspicious about the difference in what they were told.

Fourth, even if the Department chooses not to require collection of purpose information, the rule should nevertheless require disclosure of purpose information when a covered entity already has that information. We would be willing to see this disclosure limited by practical constraints so that only information collected electronically and retrievable along with other disclosable information. This principle of disclosing patient information that is available even if the rule does not require its collection is something we will repeat again in these comments. If the data exists and can be readily retrieved, then there is no reason to deny a patient the data, even if the rule does not otherwise require the collection of the data. If the rule says that a covered entity only has to disclose some elements, some covered entities will refuse to disclose other elements that are available and that could be disclosed at no additional cost.

We would support considerable flexibility in describing purpose. Purpose could be described in standard terms without using the meaningless phrase *health care operations*. Simple categories like *quality improvement*, *billing*, *licensing*, *auditing*, and more will provide patient useful information. Broad terms like *treatment* and *payment* will be adequate in many cases.

Fifth, we disagree with some statements that the Department relied upon in developing the policy here. On page 31439, these statements appear:

> In addition to the RFI, we have received anecdotal reports that identifying the purpose of a disclosure is sometimes important, but that more often individuals are most interested in learning who has accessed their information.
>
> * * * * *
>
> Of those requests, we expect that many individuals would only be interested in learning who accessed their information, without regard to why the information was accessed.

We cannot assess the Department's anecdotal reports, but our experience in dealing with consumers is that they want to know why their information was accessed. Without some indication of the reason for the access, a patient may only receive a list of names. In some instances, that list will be exceedingly long. During a hospital admission, for example, hundreds of employees may access the record of a patient, and the number of accesses will be in the thousands. Once presented with that list, patients are most likely to be confused and angry. Nearly all of the names will be unfamiliar to the patient, with only the names of a few doctors and nurses being recognized. Names of individuals who run lab tests, provide meals, prepare bills, and carry out the numerous other largely invisible functions at a hospital will not be familiar to the average patient. Many patients are likely to demand an explanation. If so, a covered entity will have to make a hard choice. It can provide the information requested on a case-by-case basis at some cost. The alternative is to refuse the patient request, making patients

both angry and suspicious. If the covered entity says that it is not required by law to provide additional information, patients will only get angrier.

We renew our suggestion that some indication of purpose be included. We renew our suggestion that purpose be disclosed if the information is readily available. We have another alternative to suggest. If purpose is not available, we recommend providing the patient with the job title or department of the employee who used the information. Since the records under consideration are all automated, marrying a list of names to a set of job titles or departments should not be complex or expensive. A patient who receives a list of names with some sense of why the recipient used the patient's information is likely to be fully satisfied. A list that says only *John Doe, Mary Roe, etc.* will be useless. A list that says *John Doe, nursing; Mary Roe, billing, etc.* will be more informative.

We repeat our view that a list of names alone will be useless to patients and detrimental to the interests of covered entities. The Department needs to find some practical (and automated) way to give patients more information about the reason for each access by the staff of a covered entity. Otherwise, patients may begin to question the actual value of electronic health care systems. We would not object if the Department adopted our suggestion for more identification of recipients but allowed a long lead time as appropriate.

We note that the Department proposes to require that an access report include a general description of the action taken by the user with respect to the record, if available, such as whether the user created, modified, deleted, or merely accessed the record. We believe that this information would be helpful to patients trying to decipher what happened to their information. However, we do not think it is a substitute for a statement of purpose or for more identification about the individuals who accessed the information. We agree, however, that address of the individual accessing the information is not likely to be meaningful.

D. Asymmetric Applicability of Rules

In numerous places both in the existing accounting rule and in the broader NPRM, the Department carefully picks and chooses among activities that would be subject to accounting and access report rules. One type of disclosure would be subject to accounting to the patient while another type would not. The resulting requirements are haphazard at best, offering the appearance of Swiss cheese, a seemingly solid mass with numerous unpredictable holes of varying dimension. We question the wisdom of this.

In the more automated systems of the future, having to support distinctions between fundamentally similar disclosure activities will be more expensive than a simple and universal rule. A rule that says keep track of *all* disclosures and *all* uses will be simpler to implement, less confusing, and less prone to error. With a simple and universal policy, no one will have to pause and make a decision whether accounting is necessary, whether a particular activity is required by law or just allowed by law, or whether a particular disclosure also requires a purpose to be recorded. In the end, a universal rule will be less expensive to implement and less expensive to operate. We suggest that the Department reconsider to the greatest extent possible the numerous exceptions and eliminate as many as possible.

We want to make clear, however, that we accept the policy that limits access accounting to electronic records only. We recognize that mandating accounting for use of paper health records is just too expensive and too cumbersome.

E. Time Period for Accounting and Access

We do not object to the establishment of a standard period for providing accounting and access information to a patient. We would be happier with period longer than three years, and we are not convinced that the costs will be significantly higher if the period were six years. We do note that the statute says three years, and we concede that having a uniform period makes sense.

We would like to suggest that the Department require covered entities to provide accounting and access information for a period beyond the mandatory three year period if the information is readily available at no additional cost. We envision that in many instances, a covered entity will have a system that will enable it to retrieve accounting and access information for any period at the same cost as for three years. The information may exist and be retrievable because the covered entity needs it for its own internal purposes having nothing to do with the HIPAA rule. When that is the case, we believe that the rule should require a covered entity to provide the information if the patient wants it. If there are additional costs, it would be fair to pass them on to the patient.

F. Concern about Electronic Designated Record Set Language

The Department proposes to limit the right to an access report to protected health information about an individual that is maintained in an electronic designated record set (DRS). We have a general concern here. When records are electronic, we wonder if the concept of a *designated record set* will continue to be meaningful. A covered entity may maintain its electronic records in a general purpose database and retrieve the information as needed for various purposes. The old, paper-based model of distinct physical records maintained in different locations – which formed the basis for the DRS concept in the first place and which appeared to have reasonable justification when first adopted – may not be valid in the future.

If so, then categorizing records as a DRS or otherwise based on purpose is either meaningless or an invitation to mischief (e.g., leading to unreasonable denials of accounting records on the grounds that the records are not part of a DRS). We admit to some uncertainty on this point, and we identify this issue as a possible concern for the future. If our suspicions about mischief turn out to be true, then there may be a need to revisit the electronic DRS notion and the limitation of accounting to DRS.

G. Suggestion Regarding Listing Disclosures Subject to Accounting in the Rule

The Department proposes to change the language in the rule from the current language which identifies disclosures exempt from accounting to new language that identifies the disclosures subject to accounting. This is principally a technical matter that is not a major change, but we have an alternate suggestion.

Any list of regulatory items that requires the reader to turn to another part of the rule to see what is included or excluded is troublesome and unclear. We gently suggest that the accounting regulation should expressly list in the rule *both* the disclosures for which accounting is required and that for which accounting is not required. The extra few lines that this will take in the rule itself will save every reader some time and effort. The cost to the Department is a few dollars for charges for printing a few more lines in a Federal Register notice. The Department's obligation to provide a readable regulation suggests that the minor expense is worthwhile.

H. Accounting for Impermissible Breach Disclosures

We have trouble making much sense from the Department's proposal to exempt from accounting any impermissible disclosures if a covered entity has provided a breach notice. First, a covered entity will have to maintain accounting for impermissible disclosures that do not require a breach notice. The Department proposes that a more serious improper disclosure should not require an accounting. That result just seems odd and wrong.

Second, any covered entity will have to keep records of impermissible disclosures anyway for its own internal purposes. Making that information available to a patient should not be complex or expensive given the basic accounting requirement for many disclosures.

Third, the premise of the exemption is that the covered entity has sent a breach notice to the patient so the patient has actual notice. However, a covered entity has no way to know if the patient actually received that notice. A patient who moved and or who did not receive the notice for another reason will expect to find the information in the health record of the entity that made the breach. Even a patient who received the notice (and breach notices are becoming quite commonplace today) may not remember it two years later. The covered entity that sent the notice will have the information anyway, and that central accounting record will remain useful to all.

Fourth, we repeat the comment we made earlier about a "Swiss cheese" or asymmetric requirement. Exempting this disclosure or that disclosure from the accounting requirement is a poor choice for the reasons we stated already, and this particular exemption makes little sense. For example, if a covered entity hires a third party to help with the breach notice – and this is quite likely in most cases – there will have to be an accounting for that disclosure anyway. We just do not see that the "savings" here are likely to be meaningful for anyone, and the information has the potential to be valuable to patients, particularly those who are victims of medical identity theft.

I. Public Health Exemption

The Department requests comment on broadening accounting exemptions for public health disclosures. In general, we oppose new exemptions for public health disclosure accounting. The first reason is the expansion of exemptions in a scattershot fashion that only serve to make the rule harder to understand and apply. We thus very strongly agree that "the complexity of carving out such public health disclosures would lead to too much confusion among individuals and covered entities" (p. 31431).

Second, for this same reason, we also reject the proposed exemption for abuse or neglect reporting. There is an existing procedure to cover concerns about disclosure to an abuser, and we would not object to tweaking that procedure if justified. We are not persuaded about "potential harms" (p. 31431) that may arise in these cases. A health record is certain to contain a non-accounting notation about any abuse or neglect disclosure, and that information will still be available to the patient or patient representative. We do not understand what a new accounting exemption will accomplish here.

Third, the Department is a major public health agency, and for the Department to change the rule without statutory direction in a way that makes disclosures to public health agencies less transparent and less accountable is quite troublesome, and not only for the conflict of interest present when the Department writes a general rule that affects the Department. A public health agency has the authority to affect the liberty and privacy of individuals in ways that equal or in some cases may exceed the authority of the police. When a covered entity shares patient information with a public health agency at any level of government, the disclosure is not likely to be expected by the average patient. This conclusion is precisely the same, whether the disclosures are required by law or merely authorized by law. Our point here is clearly much broader than the abuse reporting provision alone.

Fourth, the Department states that "such disclosures may be of limited interest to individuals and/or because accounting for such disclosures may adversely affect certain population-based public health activities, such as active surveillance" (page 31431). We reject both reasons. The Department has no factual basis for concluding that these disclosures are of limited interest. Given the powers of public health agencies, we believe that these disclosures could easily be of greater interest.

Further, we do not believe that that Department can merely assert without any justification or support that some disclosures are of less interest and others are of greater interest. This type of assertion is the regulatory equivalent of pulling oneself up by his own bootstraps. We believe that determinations of interest must be left to each individual. It is not a coincidence that when the NPRM needs a reason to support a change in the absence of clear evidence, the NPRM relies – as it does here – on a conclusion that individuals do not care about a particular disclosure. Where were the facts upon which this conclusion was based? This is a troubling pattern in the NPRM.

Finally, with respect to active surveillance, we note that public health surveillance activities have been controversial for decades. See generally SEARCHING EYES: Privacy, The State, and Disease Surveillance in America. Amy L. Fairchild, Ronald Bayer, James Colgrove (University of California Press, 2007). Hiding public health surveillance from public notice is not the way to broaden public understanding and support. The problems and conflicts are there, and they cannot be evaded or hidden for long. The Department needs to take the long-term perspective here.

J. Other New Exemptions

The Department requested comment on whether certain categories of disclosures that are currently subject to the accounting should be exempted.

1. Coroners, Medical Examiners, Funeral Directors Should Not Be Exempted from the Accounting Rule

There should be a very good reason to vary from a universal accounting rule. We find no justification for a change in the current rule here. There is no evidence offered that a new exemption would save significant costs or that training employees about a reversal of policy would not be more confusing than the existing policy. We observe that the Department proposes no other exemption for disclosures about the deceased, and it does not offer a justification for this exemption other than an assertion that these disclosures are relatively routine, expected, and do not raise significant privacy concerns.

We disagree with all of these reasons. We do not believe that most individuals have any idea about these post-death disclosures, and there is no factual basis to say that the disclosures are expected. We concede that the privacy interests in the case of those who are deceased may be lessened. However, that does not mean that there will not be significant privacy concerns in the case of individuals who died of AIDS, committed suicide, had a genetic disease or condition, or suffered from other health conditions that families would not be happy to share.

The Department observes for the entire class of would-be accounting exceptions that "to the extent such disclosures are made through direct access to electronic designated record set information, such disclosures will be recorded and available to the individual in an access report under proposed § 164.528(b)" (p. 31432). We cannot tell if the observation is relevant to this particular class of disclosures, but if it is, the result would be that similar activities would result in accounting records in some cases and not in others. This will only breed confusion among covered entities and provide misleading information to patients.

We also note that the recipients of information under this exemption are not subject to HIPAA, and ***they are free to redisclose the information without sanction under HIPAA***. An accounting of the original disclosure may be the important to tracing subsequent misuse. Having said all this, we admit that we find the stakes in this exemption to be lower than in some other proposed exemptions.

2. Cadaveric Organ, Eye, or Tissue Donation Purposes

The Department justifies this proposed change in policy "to avoid putting covered entities in the position of having to request consent from grieving families with respect to donation of organs of a deceased loved one before a determination has been made that donation would be medically suitable" (p. 31433). Given the strong policy arguments for organ donation, we would be more inclined to agree with the proposed exemption if the reason the Department suggested actually made any sense.

The current rule already allows for *non-consensual* disclosures for organ donation purposes. Since there is no need to obtain consent for disclosure before or after there has been a determination that organs would be suitable, the Department's justification is hard to understand. Consent is needed for an actual organ donation, an action that can be difficult with grieving families, but that is something not covered by the privacy rule. The Department did not even argue that the current requirement for accounting for an organ donation disclosure is a problem or a barrier to organ donation. We also note that the recipients of information under this exemption are not subject to HIPAA so further controls over use of the information by the recipients is absent. As a result, we see no reason at all for the proposed exemption.

3. Disclosures for Protective Services for the President and Others

The existing provision that allows non-consensual disclosures for protective services requires no court order, procedural prerequisite, or even a paper request. Disclosures of highly sensitive health information can be made on oral representations by a wide range of law enforcement personnel. The accounting requirement is the only record that a disclosure was made. We find nothing in the NPRM that hints at a justification for this exemption or that suggests that the current exemption is a problem.

We fear that with electronic health record systems, those providing protection services may have untrammeled access to the systems and the ability to look at any record they want without a request, gatekeeper, or any limitation. Accounting for all disclosures is the only hope to limit misuse of the basic nonconsensual disclosure authority. We also note that the recipients of information under this exemption are not subject to HIPAA so further controls over use of the information by the recipients is absent. As a result, we oppose the proposed exemption.

4. Strongly Oppose Health Oversight Activities Exemption

We oppose this proposed exemption to the current accounting requirement. The Department argues that health oversight disclosures "primarily are population-based or event triggered and thus relate to the covered entity, rather than the individual (if an investigation is focused on the individual rather than the covered entity, then the Privacy Rule at § 164.512(d)(2) generally treats the investigation as for law enforcement rather than health oversight, which means that the disclosure would be subject to the proposed accounting provision)" (p. 31433). The Department's justification is hard to accept and relies on information that is not known at the time of disclosure.

The number of disclosures that are made for health oversight activities can be extremely large, up to and including all health records of a health care provider. Many health oversight disclosures will be indistinguishable from other disclosures that are subject to accounting, and it will be hard for covered entities to know how to characterize a request. In too many cases, it will be necessary to seek legal advice. If so, then the result will be to delay disclosure and add to its cost.

Second, we repeat our previous comment about the conflict of interest present when the Department writes a general rule that affects the Department. Many of the disclosures made for

health oversight purposes are to the Department, and it is just *too convenient* for the Department to change the rule so that it does not apply to its own activities. We think this change should require a much higher burden of proof. We see little factual justification in the NPRM.

Third, it is fine to say that the disclosures are population based while disclosures for law enforcement focused on the individual would be subject to accounting under another provision. These statements are substantially misleading. We begin by noting that recipients of information under this proposed exemption are not subject to HIPAA so further controls over use of the information by the recipients is absent. Accounting is an important constraint both on the recipient and on the discloser. We further observe that a population based request can easily turn its focus on a specific patient who told a physician about illegal activities (e.g., drug abuse) that the patient engaged in. We have yet to meet a policeman, fraud investigator, or Inspector General who says that they will not use information about illegal patient conduct to prosecute the patient no matter how the information was originally obtained. They do not care if the original disclosure was population based or otherwise. HIPAA offers no protections for patients when information is shared in a population-based disclosure.

Fourth, the proposed exemption would place a covered entity in an impossible situation. How does the covered entity know whether the request is population based or focused on an individual? Investigators typically demand records without revealing their purpose or the scope of their investigation. Indeed, in many cases, investigators will not know in advance just what they are looking for or expect to find. The confusion and consultation that will be needed to determine if an accounting is actually required will take more time and effort than the accounting itself.

Fifth, we observe that accounting for large-scale disclosures in an electronic health system should be easy, inexpensive, and effortless. We see no reason to exempt health oversight disclosures of records from any electronic health systems that have an accounting capability. If the Department wants to exempt health oversight disclosures from paper records only, that new exemption would not address our concerns, but it would limit the damage.

5. Oppose Changes in Research Accounting

The Department is considering changing the requirement for accounting for research disclosures. We strongly oppose any change at this time.

First, the existing rule already has an alternate procedure – a protocol listing – that addresses the problem of providing an accounting when many records are disclosed. There is no evidence that this procedure is inadequate to deal with concerns about cost or convenience. We do not think that the protocol listing provides an adequate privacy balance. We would prefer full accounting for *all* research uses and disclosures. We believe that in the coming electronic health information environment, it will be simple and inexpensive to provide universal accounting for research. We would not object to a proposal that would defer full accounting requirements until the computer systems are in place to accomplish the accounting at little cost. However, if the Department takes accounting for research off the table today, it will never be able to reimpose the requirements

even if accounting can be accomplished at no meaningful additional cost at all. We urge the Department not to foreclose that possibility.

Second, the use of patient records for research – something we generally support – is highly controversial with the American public. Every public opinion poll for decades shows that patients want to be asked for consent for the use of their health records for research. We do not propose that the Department accede at this time to those public demands. We do think, however, that the Department must take note of public opinion here.

If the Department goes too far and makes it impossible for patients who care to learn how their health records have been disclosed for research, it will only be a matter of time (and a high-profile scandal or two) before public demands for consent are met by a Congress that shares the same views on this subject as the public. If put to a vote, Members of Congress would readily vote to require patient consent (or perhaps even more). That vote may happen sooner than otherwise expected, as it may only take a single security breach by a researcher conducting controversial and unpopular research to put the issue on the front page of every newspaper and news website.

Third, the privacy and the research stakes here are high. We support research and researcher access to health records under reasonable conditions. However, not all research is the same, and we do not assume that all researchers have pure and noncommercial motives. Further, there are some areas of research that are very sensitive for moral, ethical, or political reasons. If the Department removes the only method whereby a patient can learn that his or her record was used for a research project, it will have nothing to offer an aggrieved patient and will have no defense when that scandal arises.

Balancing the societal interest here and the privacy interest requires that there be some privacy control. Patients have the right to know if their records have been used for research, especially when they object to the nature of the research or the purpose of the researcher. We do not propose giving patients a veto, but denying them the information is a major restriction on privacy.

Fourth, the patient's privacy interest is as substantial in the research area as it is anywhere else. Research can delve into any and every sensitive area of medicine and can rely on any and all patient data, ranging from sex and age on one end to diagnoses, sexual preference, and genetic data on the other. It is hard to think of a more sensitive collection of information than that in a health record, and the HIPAA rule allows researchers all over the world to obtain health records, regardless of their actual privacy practices.

Fifth, many researchers who obtain records from covered entities are not themselves subject to HIPAA or to any privacy law at all. HHS has chosen not to require any basic privacy (or security) protections for records disclosed to researchers without patient consent. We believe that researcher privacy and security practices are often deficient. An accounting record is the only hope that a patient has of learning which of the patient's multiple covered entities disclosed the patient's records to the researcher. A patient generally has no privacy rights with respect to researcher records, and that is a major gap in privacy protections that HIPAA does not address.

Sixth, we observe that Congress knew about complaints from the research community about the privacy rule, and it chose not to mandate any change. The research community groans loudly about every requirement that seeks to strike a fair balance between the interests of researchers and the interests of research subjects and others. We choose not to list here the many research activities that have been found to be so unethical or so harmful as to make front-page news in every newspaper in the country. Some fraudulent research has resulted in unnecessary deaths, harm to millions, and great expense to society. We simply state that all research cannot be viewed as an unquestioned societal benefit to the extent that researchers need not be held accountable for their actions in the same way as others. Researchers do not deserve a free pass when it comes to privacy. An accounting for disclosure to researchers is a minimal step.

Seventh, in an electronic health record environment where access to a patient's record may be allowed by any of the dozens or hundreds of institutions that have access to that record, an audit trail is essential to determine who gave out the record and why. In fact, we worry that existing gatekeepers who can limit researcher access (whether because of the qualifications of the researcher, the controversial nature of the research, the lack of scientific merit, or other valid reasons) will be unable to continue to restrict access to the records that they created and that they control in the current environment. We foresee the possibility that patient information may be disclosed to researchers by anyone with access to a health computer network and without any substantive review by any covered entity. The accounting record showing who disclosed what to whom may be the only hope for accountability.

We suggest that the Department needs to consider how researcher access will be controlled in the coming health information network. We urge the Department not to make decisions today without taking a complete and long-range perspective. Accounting records may provide the only way to determine how and why a record was disclosed to a researcher.

Eighth, we observe with some amusement that the Department makes our Swiss cheese/asymmetric applicability of rules argument here in the NPRM. It says that there is the possibility that uses for research may not be subject to accounting but that disclosures would be. Confronted with this disjointed outcome, the Department seems to be leaning toward the conclusion that there be no accounting for research activities at all. Under that logic, however, the ambiguous, scattershot nature of the current accounting rule coupled with the proposed new exemptions argues for no accounting at all for any disclosure. That result is not allowed under the law, and it would be a terrible privacy policy. We would rather have accounting for research disclosures than for research uses. Disclosures are external to the covered entity and, in most instances, are made to researchers who are not subject to any oversight or privacy requirements.

Ninth, we are not at all persuaded that approval of research protocols by institutional review boards justify removing the only audit trail for researcher use of health records. The general shortcomings of the IRB process are too broad to address here. We can state, however, that most IRBs have little training in privacy, and they do a cursory job at best in evaluating projects for their privacy consequences. There are no "industry" standards for privacy (or security, for that matter), and IRBs cannot oversee the privacy practices of researchers. Approval of research projects by IRBs is no substitute for privacy protections for patients that the patients can

exercise. Further, there is the possibility that future changes in IRB rules may further weaken or eliminate the role of IRBs in privacy protection for some types of research.

Finally, we observe that the inclusion of a single line about the possibility of research disclosures in a privacy notice that few patients read or understand is no substitute for allowing a patient to know about a research disclosure if that patient wants to know. The deficiencies of privacy notices are well known, and it is hard today to suggest that a privacy notice accomplishes much of anything. We suggest that you read the recent staff report of the Federal Trade Commission on the value of privacy notices.

6. "Required By Law" Language is Not Acceptable

The Department proposes to exempt from accounting most disclosures that are required by law. We strongly oppose that change.

The Department's justifications make little sense. It is fine to suggest that these disclosures are "often" population based, but that makes little difference to the individual. If your record is disclosed, the reason does not matter because your privacy is affected nevertheless. It is not affected less because it was a population-based disclosure. This is not a Miranda situation where a notice is required only if the record will be used against the individual. At the time of the disclosure, no one can be sure if the record can or will be used in a way that is adverse to a patient. Further, in those cases when a mandated disclosure is not population based, then every individual has a heightened privacy interest. Using the Department's own standard here, the non-population-based disclosure impinges on the individual's privacy interest. Yet the proposed change in the rule ignores that individual and that circumstance altogether.

The Department argues that mandated disclosures reflect a decision by a legislature. But that says nothing other than the disclosure is mandated by law. Legislatures mandate disclosures of personal information all the time. It does not mean that the privacy interests of the individual have been fully or fairly balanced.

We point to the Privacy Act of 1974 to show that Congress took the exact opposite approach. In 5 U.S.C. § 552a(c), Congress mandated accounting for most disclosures. There is no exemption for disclosures required by law. There is only an exception for disclosures required by the Freedom of Information Act and some law enforcement disclosures. Existing congressional policy applicable to the federal government is that there is no reason to exempt disclosures required by law from an accounting requirement. The Privacy Act accounting requirement for mandated disclosures has not generated any opposition or proposals for change in nearly four decades.

The Department says that it is reasonable to assume that individuals are aware that their health information will be disclosed where mandated by law. First, we believe that statement is not true. There may be dozens of laws in each state plus numerous federal laws that mandate the disclosure of health records. We doubt that most lawyers or most HHS employees, let alone most patients, would be able to pass a test on the subject of legally mandated disclosures of health records. Second, it is irrelevant what people may or may know in the abstract. The fact that your

personal record was disclosed at a particular time and for a particular purpose is a fact that is important if you were concerned enough about your privacy to ask for an accounting record. Hypothetical knowledge is no substitute. Third, the more disclosures that are mandated, the more important that it is for there to be an accounting. The inclusion of this language invites loopholes to be created to create exemptions for accounting.

Here too, we urge the Department to take the long-range view. The electronic health care systems of the future will handle accounting with ease. This is not the time to change a requirement that the Department already mandated and that covered entities have already implemented. The Department should not stop mandating accounting that will be easier and less expensive in the near future. We do not support any change here at all, but we would hate to see a permanent change made for reasons that will not apply in a few years.

K. Administrative Changes

1. Approximate date

The Department proposes that a covered entity need only provide an approximate date or period of time for each disclosure, if the actual date is not known. We have no objection to this change, but we suggest that the exact date must be disclosed if it is known and easily retrievable.

2. Support for Name of Recipient Exception

The Department proposes an exception for providing the name of the recipient would itself represent a disclosure of protected health information about another individual. We support this change. However, we suggest that the Department make it clear that disclosing the name of a health care professional or employee of a covered entity does not qualify for this exception. We do not want to see the exception misconstrued or overused.

3. No Objection to Brief Description

The Department proposes a change to the current requirement that the accounting include a brief description of the protected health information that was disclosed. We have no objection to replacing "a brief description of the protected health information disclosed" with "a brief description of the type of protected health information disclosed." We also have no objection to the change in regulatory language from "statement" to "description" to make clear that only a minimum description is required if it reasonably informs the individual of the purpose of the disclosure.

4. Support for Limiting Accounting Disclosures

The Department proposes to allow a covered entity to give individuals the option of limiting the accounting to a particular time period, type of disclosure, or recipient. We support this change.

5. No Objection to Time and Format

The Department proposes to (1) decrease the permissible response time from 60 days to 30 days; (2) require that covered entities provide individuals with the accounting in the form and format requested by the individual if readily producible (e.g., an electronic copy of the accounting); and (c) clarify that the covered entity may require the individual to submit the accounting request in writing. We have no objection to these changes. The Department also proposes that the covered entity provide the access report in a format that is understandable to the individual. Of course, we support that proposal.

6. Effective Dates

Everything always takes longer than expected. We do not object to extended periods for compliance with new requirements.

7. Suggestion Regarding Notice of Privacy Practices

The Department proposes methods for covered entities that must prepare a revised notice of privacy practices and provide the notice to patients. Frankly, the written notice is of so little value to patients that we support any reasonable method that minimizes the cost to covered entities of providing revised notices. However, we do suggest that covered entities be required to ***post revised notices on their websites no later than the effective dates of the new requirements***. The website can explain why the written notice a patient has and the website notice are different.

L. Strong Support for Business Associates Change

The Department wants to exercise its general authority under HIPAA to propose that the covered entity's access report include uses and disclosures by business associates of electronic designated record set information maintained by the business associates, rather than merely providing a listing of business associates. We very much support this decision. We agree with the Department that the statutory alternative to provide a list of business associates is terrible for patients, for covered entities, and for business associates. If only a few patients who were given listings of business associates sought to follow up with the business associates, the burden on everyone would be enormous and disproportionate to any benefit. We believe that the statutory provision for a list is well intentioned, but it is not practical.

M. Health Information Exchanges Should be Subject to Robust Accounting

The NPRM states that HHS considered providing individuals with the right to receive a full accounting for treatment, payment, and health care operations disclosures when such disclosures are made through an electronic health information exchange. However, the Department states that it concluded that disclosures would be overly burdensome compared to the benefit to patients. We disagree.

We strongly object to the position the Department has taken on leaving out HIE systems from robust and complete accounting requirements. If a patient record is moving through an HIE, then the HIE should be subject to the same accounting standards that extend to HIPAA-covered entities. We note that HIE systems are coming online at a rapid rate, and that many patients' records already flow through some form of these systems. These systems are generally opaque to patients, and the Department has now abridged the rights of patients to retrieve information from these systems, which may well be integral to treatment, payment, and/or health care operations.

It can be argued that in the very near future, HIE systems will have more patient information flowing through them than through the systems of the providers where treatment has originated. In the coming networked and honeycombed health care infrastructure, it will be (and already is) essential for patients to be able to track their information. In the online world outside of health care, we already see that advertisements served to consumers on web sites are part of an improbably complex digital ecosystem where consumers are left in the dark about what entity is receiving, transmitting, serving, storing, or using information. It is incorrect policy for HHS to allow a similarly opaque digital ecosystem to build up in the health care arena. We understand that the HIE ecosystem is going to be necessarily complex, but anything that helps patients figure out what happened to their information and that makes users accountable for their information activities is especially valuable. We understand that HIEs come in many flavors and architectures, with potentially substantially differing data flows. This makes it all the more important to have some type of accounting rules apply to these entities.

We reiterate that the Department needs to adopt a forward-looking rule on accounting that takes into understanding that some HIE systems will ultimately contain more patient information than providers themselves currently have, and that in fact, patient access to HIE accounting will likely be more important than the Department is foreseeing. If a patient's information is in an HIE system, and there is a breach, or there are problems or a need to find where, how, and why information was disseminated, there may be no mechanism for patients to learn what happened and who is responsible. It is not appropriate to leave this up to the goodwill of each individual HIE. A patient's rights may vary from place to place in ways that are wholly inexplicable to the patient. A robust accounting rule will encourage well-behaved HIEs.

We appreciate that HIEs will need to adopt certain standards to comply. We support a long deadline for adoption. But to err on the side of leaving HIEs out of accounting with some small exceptions is the wrong policy and will result in poor practices and less privacy. There is every likelihood that states will begin to enact a patchwork of laws to cover the problems that will arise in this area, which will in the end complicate matters for providers, HIEs, and patients alike. This outcome can be avoided with a proper policy from the outset.

N. Two Additional Suggestions on Focus Groups and Accountability Formats

We would like to offer a general suggestion. Because we all have so little experience with the use of accounting by patients, we think that it would be useful for the Department to explore this subject by sponsoring focus groups or other data collection methods. Usage information could also be collected from personnel at covered entities that have experience under the existing rule with providing accounting records to patients. It is too late for the Department to do so in advance of this rulemaking, but it would be useful in several ways for the future.

First, we could all learn more about what patients want. Second, we could learn how patients use or would use accounting records available to them. Patients would likely have several different patterns of usage. Some would be generally interested in how their records flow through the health care system. Some would want to know if specific individuals known to them accessed their records. Some would use accounting records to find possible leaks of their records. Some would use accounting records for other purposes that we cannot envision. The way that patients use or might use accounting records is not likely to be static and may evolve over time..

We also think that the Department could help everyone by offering (not as part of this rulemaking) several different formats for the disclosure of accounting records to patients. The same groups (patients and professionals) that we just suggested might help to identify the formats that would make accounting records most useful to patients. We suspect that several different formats might be identified. We do not look for a mandatory format requirement from this process, but if the Department would do some basic public opinion research, everyone would benefit. Likely outcomes would include better guides for patients, more choices for patients, clearer guidance for software developers, and lower costs for everyone.

Thank you for the opportunity to submit comments.

Pam Dixon,
Executive Director, World Privacy Forum
www.worldprivacyforum.org