WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

Regarding Department of Health and Human Services, Agency for Healthcare Research and Quality, Office for Civil Rights *Notice of Proposed Rulemaking on Patient Safety and Quality Improvement, 42 CFR Part 3* (RIN 0919–AA01)

Center for Quality Improvement and Patient Safety
Attention: Patient Safety Act NPRM Comments
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Via overnight mail and the Federal Rulemaking portal

Re: Comments of the World Privacy Forum, Department of Health and Human Services, Agency for Healthcare Research and Quality, RIN 0919–AA01

April 4, 2008

The World Privacy Forum welcomes the opportunity to comment on the Department of Health and Human Service's Notice of Proposed Rulemaking on Patient Safety and Quality Improvement (RIN 0919–AA01). The notice appeared at 73 Federal Register 8112 (Feb. 12, 2008).

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

Our comments and recommendations focus on several aspects of the proposed rulemaking. Notably, we discuss issues regarding the proposals for FOIA, required certification regarding seven Patient Safety Organization (PSO)[1] criteria, patient safety activities, disclosure of nonidentifiable patient safety work product -- including disclosures to the Food and Drug Administration, law enforcement, and business operations -- continued protection of patient safety work product, and overall enforcement of the final rule.

[1] A *Patient Safety Organization* is a term of art defined in the NPRM as a "private or public entity or component thereof that is listed as a PSO by the Secretary in accordance with proposed § 3.102." The term *Patient Safety Organization* will hereafter be noted in these comments as PSO.

I. Freedom of Information Act

In several places, the Notice of Proposed Rule Making (NPRM)[2] discusses the use of Freedom of Information Act (FOIA) criteria with respect to public disclosure of information about the Patient Safety Act operations and its administration by the Department. The NPRM discusses the FOIA in connection with:

- Subpart B — PSO Requirements and Agency Procedures (page 8126), relating to disclosure by PSOs of potential conflicts of interest with their provider clients.

- Proposed § 3.104(c) — Actions Regarding Required Disclosures by PSOs of Relationships With Contracting Providers (page 8133), relating to evaluation of required disclosure statements

The World Privacy Forum is a strong supporter of the FOIA, but this is not the place to rely on its standards alone. The FOIA is an all-purpose law that establishes baseline standards for the disclosure of government documents. It does not limit the ability of an agency to disclose information on its own motion, to satisfy its statutory disclosure obligations, or to meet public needs.

The most troubling aspect of proposed reliance on the FOIA is that it may be read to limit the discretion of the Secretary to make disclosures not required by the FOIA. Patient Safety Organizations or others seeking to hide patient safety operations may try to rely on exemptions in the FOIA – particularly those relating to confidential business information – to hide from the public information that is of public interest and that should be disclosed by the Secretary.

The intent of the proposed rule with respect to affirmative disclosures by the Secretary is not as clear as it could be, or needs to be. We suggest that the rule or the commentary be revised so that it states expressly that the Secretary retains the authority other than the FOIA to determine affirmatively what information should be made available to inform the public about the operations of the Patient Safety Act, about those entities that are regulated by it, and about the Department's implementation of the Act.

II. Proposed § 3.102(b)(2) — Required Certification Regarding Seven PSO Criteria

We have recommendations for three parts of the proposed section 3.102 (b)(2). Our comments focus on patient identifiers, providers, and collecting data in a standardized manner.

A. Patient Identifiers

Contracts between a PSO and a provider must meet specific minimum requirements. On page 8128, the NPRM provides:

[2] *Notice of Proposed Rule Making* hereafter noted as NPRM.

> If they choose to do so, providers and PSOs may enter into contracts that specify stronger confidentiality protections than those specified in this proposed rule and the Patient Safety Act (section 922(g)(4) of the Public Health Service Act, 42 U.S.C. 299b–22 (g)(3)). For example, a provider could choose to de-identify or anonymize information it reports to a PSO.

This provision does not go far enough to protect patient privacy. Any sharing of patient data, no matter what the purpose is, directly affects the privacy interest of patients. The individual at the PSO who reviews a patient's file could be that patient's brother-in-law, neighbor, college roommate, or any other individual who knows the patient or the patient's family, coworkers, or friends. Even if the PSO does not have direct knowledge of the individual, many people have some biographical information online at this point, and some peoples' identities, are in essence, a click or two away. Recent articles about large institutional health care providers with audit controls in place having difficulties with inappropriate access to celebrities' health care files points to the scope of the challenges here and the need for express protections for this information.[3]

Especially when public policy requires the sharing of patient data for a purpose unrelated to the treatment of that patient or the payment of that patient's bill, all reasonable steps should be taken to lessen the chance that a patient will be identifiable to someone who sees the data. Removal of identifiers should not be left as a choice to be made or not made by PSOs and providers, neither of which have a natural incentive to expend resources to protect patients whose records are used in patient safety activities, especially if HHS only pays lip service to stronger protections.

We ask that the rule expressly mandate that all patient data be de-identified or anonymized to the greatest extent possible and at the earliest possible opportunity consistent with the ability of the PSO to carry out its operations. Specifically, any patient data transferred by a provider to a PSO should be de-identified or anonymized unless the provider and the PSO jointly determine that identifiers are necessary. The privacy officer of the provider and the PSO should be involved in the determination.

In addition, a PSO should be required to de-identify or anonymize identifiable patient data as soon as identifiers are no longer necessary for the PSO to carry out its operations. Where there is justification for transferring patient data in identifiable form, the justification for retaining identifiers should be documented and retained. Further, a review of the continuing need for identifiers should be required every three months, and there should be a presumption that any data not in active use should be de-identified or anonymized six months after transfer to the PSO. Finally, PSOs that receive or create de-identified or anonymized patient data should be contractually required not to attempt to re-identify the data.

Patient privacy should not be left to the parties to address at their whim. It is too easy for the parties to overlook patient privacy and to decide that it is not in their interest to bother to de-

---

[3] See for example: Charles Ornstein, Los Angeles Times, *Fawcett's cancer file breached: The incident occurred months before UCLA hospital employees were caught snooping in Britney Spears' files*. April 3, 2008. See also: Associated Press, *UCLA Medical Center fires employees for snooping into Britney Spears' medical files*, March 15 2008.

identify or anonymize patient data. That is why the rule should mandate de-identification or anonymization.

B. Providers

On page 8128, the NPRM also addresses the definition of provider:

> We note that the Secretary proposes to exercise his authority to extend the definition of ''provider'' for the purposes of this statute to include a provider's ''parent organization'' (both terms are defined in proposed § 3.20). This proposed addition is intended to provide an option for health systems (e.g., holding companies or a state system) to enter system-wide contracts with PSOs if they choose to do so. This option would not be available in the absence of this provision because the parent organizations of many health care systems are often corporate management entities or governmental entities that are not considered licensed or authorized health care providers under state law.

This is unobjectionable. However, the use of the term *provider* in an environment where the term *health care provider* is already an established term under the HIPAA health privacy rule will engender confusion when the two terms have different scopes. At a minimum, we think that it would be appropriate for the commentary accompanying the final rule to address the two terms, emphasize the differences, and clarify the obligations.

C. Collecting Data in a Standardized Manner

On pages 8128 and 8129, the NPRM discusses "formats and definitions that would facilitate the ability of PSOs to aggregate patient safety work product." This is unobjectionable, but this work should be done with due regard to patient privacy. That may mean that the standards should provide, whenever possible, for *more* de-identification or anonymization, mandate the collection and retention of *fewer* data elements that assist re-identification, and require the use of creative statistical techniques that can preserve the utility of information while making identification or re-identification more difficult. We note that the ability to identify individuals from a handful of non-unique identifiers increases all the time. More than 80% of individuals can be uniquely identified from birth date, five digit zip code, and gender.

In developing these standards, we hope that the Department will reach out to internal and external experts in this area and will affirmatively seek to engage privacy and patient groups in developing standards. Just talking to the health industry will not produce a result that fully reflects the privacy and other interests of patients.

III. Proposed § 3.206(b)(4)—Patient Safety Activities

A. Data Sharing

On page 8145 and 8146, the NPRM discusses sharing of data between providers and PSOs:

> Balancing these concerns, we are proposing that other than the reporting relationship between a provider and a PSO, PSOs be permitted to disclose patient safety work product to other PSOs or to other providers that have reported to the PSO, and providers be permitted to make disclosures to other providers, for patient safety activities, with provider and reporter identifiers in an anonymized (i.e., with certain direct identifiers removed, but not nonidentifiable under the proposed rule) or encrypted but not fully nonidentified form. For patient identifiers, the HIPAA Privacy Rule limited data set standard would apply. See 45 CFR 164.514(e).

Any type of data sharing can be troublesome, even when direct identifiers are removed. For patient information, the sharing of a limited data set as proposed should be accompanied by a requirement to comply, at a minimum, with the requirements established in the HIPAA privacy rule for a data use agreement. 45 CFR 164(e)(4). The data set agreement provides important privacy protections for individuals, and those protections should be mandatory for any sharing in a PSO context. The proposed rule should be amended to expressly require the use of data use agreements for any data sharing.

In addition, **a PSO should be required to maintain an accounting for any disclosure of identifiable patient information that it makes**. We would prefer that an accounting requirement cover *all* disclosures without exception. Auditing technologies allow for this level of robust auditing now, and it would serve to increase patient trust of the system if patients were allowed to see all disclosures. We would understand if the Department chooses to require an accounting of disclosures that paralleled the HIPAA privacy rule requirement.

However, either way, there needs to be a requirement for the PSO to maintain an accounting of disclosures at least equal to the HIPAA privacy rule requirement. Patients must be able to use this accounting for uncovering data breaches and other unauthorized accesses that could lead to medical identity theft, which poses significant safety risks to patients.[4]

B. Private Agreements

The NPRM (page 8146) allows providers and PSOs to impose greater confidentiality requirements through private agreements.

> Moreover, providers and PSOs are capable of imposing greater confidentiality requirements for the future use and disclosure of the patient safety work product through private agreements (see section 922(g)(4) of the Public Heath Service Act, 42 U.S.C. 299b–22(g)(4)). However, we note that the government would not be permitted to apply civil money penalties under this Part based on a violation of a private agreement that was not a violation of the confidentiality provisions.

[4] For more on medical identity theft, see the World Privacy Forum report on medical identity theft, *Medical Identity Theft: The Information Crime that Can Kill You*, May 2006. <http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>.

This is fine as far as it goes. However, since the NPRM says expressly that there will be no enforcement of these agreements by HHS, the rule should be amended to require expressly that these agreements state that patients are third party beneficiaries of the agreements. If HHS cannot enforce a confidentiality provision and if patients cannot enforce it either, then the agreement may be meaningless because the parties can violate it without any real consequence.

Adding third party beneficiary language will open up or ease enforcement under state laws. Indeed, the WPF believes that patients should be third party beneficiaries of all confidentiality contracts and agreements required by or permitted by the PSO rule. The ability of patients to look after their own confidentiality interests would be a valuable supplement to what we predict will be enforcement by HHS that is no more aggressive than the enforcement of the HIPAA privacy rule. We recommend that the rule be amended to expressly provide that patients must be third party beneficiaries of all confidentiality agreements under the rule.

C. Amending the Definition of Health Care Operations

On page 8146, the Department seeks comments on the advisability of amending the definition of Health Care Operations in the HIPAA privacy rule. We believe that such an amendment is essential to clarify the terms under which patient safety reporting is permissible. Unless the Department specifies limits on PSO disclosures directly in the HIPAA rule, there is too great a possibility that covered entities will be confused or will interpret the definition too loosely or too narrowly.

We see no reason to have the lawyers for every covered entity that hires a PSO to have to make the same determination about the scope of permissible disclosures. Indeed, having raised the question, it seems to us that the Department is virtually obliged to change the definition to conform. Failure to make the change will be an open invitation to mischief or confusion. The Department should amend HIPAA at the same time that it finalizes the PSO rule.

IV. Proposed § 3.206(b)(5)—Disclosure of Nonidentifiable Patient Safety Work Product

A. Contextually Nonidentifiable

The discussion in the NPRM beginning on page 8147 about nonidentifiable data is adequate with respect to patients.

> Therefore, where patient safety work product contains individually identifiable health information, that information must be de-identified in accordance with 45 CFR 164.514(a)–(c) to qualify as nonidentifiable patient safety work product with respect to individually identifiable health information under the Patient Safety Act. We propose that patient safety work product be contextually nonidentifiable in order to be considered nonidentifiable for the purposes of this rule. Contextual nonidentification of both providers and reporters would match the standard of de-identification in the HIPAA Privacy Rule.

By sticking to the standard in 45 CFR 164.515(a)-(c) (and excluding the alternate limited data set provisions in (e)), the NPRM applies a standard for patients that is consistent with the HIPAA privacy rule. That is helpful.

However, we are troubled by the phrase *contextually nonidentifiable*. We do not know what the phrase means, and we are worried that it will be applied in other places and in other ways for mischievous purposes. Establishing standards that distinguish between identifiable and non-identifiable data is extremely complex as a matter of law and policy. We refer you to *Opinion 4/2007 on the concept of personal data* from the Article 29 Working Party, <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf>. The Article 29 Working Party was established by the European Union under the terms of its data protection directive. Another source on the subject is Appendix A, *Privacy for Research Data*, Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data, National Research Council, Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data (2007), <http://books.nap.edu/catalog.php?record_id=11865>.

The last thing that the complex and badly defined field of identifiability of personal data needs is a new and vague phrase, especially as applied to health care. The term *contextually nonidentifiable* is not in common use. An Internet search found no uses of these words other than the NPRM reference. Worse, an exhaustive Lexis/Nexis and Factiva database search found no other uses of this term, other than the NPRM publication in the Federal Register.[5] A search of law reviews for all dates similarly turned up no use of the term. The term also does not appear in Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), the federal government's main statistical confidentiality law.

We strongly urge the Department to drop the words *contextually nonidentifiable*. We do not necessarily object to the broader intent here, although we admit to not fully understand what the Department is driving at. The words *contextually nonidentifiable* add nothing to the discussion and will only engender confusion. Worse, the term *contextually nonidentifiable* is highly likely to lead to problems due to the lack of precise definition, due to the lack of support for the term generally, and especially the lack of support in key Acts such as CIPSEA.

B. Provider Identification

The same protections that we have proposed for patients should apply to providers (page 8147). If provider data is disclosed in circumstances in which there is *any* doubt about the possibility of identification or reidentification, the disclosures should be accompanied by data use agreements that expressly prohibit any further disclosures or attempts at reidentification. Further, the rule should expressly state that providers whose information is disclosed are third party beneficiaries of any data use or other agreements involving the disclosure of provider data.

---

[5] Exhaustive Factiva database search conducted April 3, 2008 using the widest possible parameters and searching for all dates. Exhaustive Lexis/Nexis database search conducted April 3, 2008 with parameters allowing information for all possible dates to be located for all documents in English. Internet search conducted week of March 18 and repeated April 3, 2008 using major Internet search engines.

V. Proposed § 3.206(b)(7) — Disclosure to the Food and Drug Administration and FDA-Regulated Entities

The World Privacy Forum does not offer an opinion about the authority of the Department to extend the statutory disclosure authority for the FDA to cover FDA-regulated entities. However, we do have an opinion on the conditions that should attach if these disclosures are allowed. On page 8149, the NPRM states:

> We further propose at § 3.206(b)(7)(ii) that the FDA and entities required to report to the FDA may only further disclose patient safety work product for the purpose of evaluating the quality, safety, or effectiveness of that product or activity; such further disclosures are only permitted between the FDA, entities required to report to the FDA, their contractors, and disclosing providers.

The disclosure limitation is reasonable. However, the limitation only addresses *disclosure* and not *use*. **It is crucial that the use of the information by FDA-regulated entities be limited to the stated purposes of the Act**. A pharmaceutical manufacturer should not be able to use the information to engage in any activity related in any way to marketing, marketing research, or patient profiling. We have already witnessed FDA-mandated drug safety programs allowing such marketing to occur, for example, in the iPledge program.[6]

The proposed rule should be amended to expressly prohibit any use of data for marketing or any other purpose not expressly permitted by law. The same standard may be appropriate as well for other activities related to providers. If the Department chooses to stretch the statute to allow these disclosures, the reporting of safety information to FDA-regulated entities should not provide an opportunity for anyone to create, enhance, or otherwise exploit the information for marketing.

VI. Proposed § 3.206(b)(9) — Disclosure to Business Operations

In discussing the disclosure of information by providers and PSO, the NPRM states on page 8151:

> Nonetheless, we expect that providers and PSOs who disclose privileged and confidential information to attorneys, accountants or other ethically bound professionals for business purposes will engage in the prudent practice of ensuring such information is narrowly used by the contractor solely for the purpose for which it was disclosed and adequately protected from wrongful disclosure.

---

[6] See World Privacy Forum statement to the FDA Dermatologic and Ophthalmic Drugs Advisory Committee and the Drug Safety and Risk Management Advisory Committee, *Privacy and the iPledge Program*. August 1 2007. Testimony available at <http://www.worldprivacyforum.org/pdf/WPF_FDAiPledge_08012007fs.pdf>.

The Department's expectations are not reassuring. We choose not to list here the large number of lawyers, accountants, and other professionals who have been found guilty in recent years of not complying with their legal and ethical obligations. We see no reason why disclosures to professionals for PSO activities should not be regulated just as the disclosures are regulated under HIPAA. This presents a substantive loose end in the proposed regulation.

For disclosures of patient information to the same class of professionals under HIPAA, a business associate agreement is a legal requirement. The patient safety rule should be amended to require the same type of agreement for patient safety information. We can see no reason to rely on mere expectations when the terms of use and disclosure can be expressly spelled out.

Indeed, failure to require the equivalent of a business associate agreement will only lead to confusion. A provider may disclose patient information to an accountant under HIPAA pursuant to a business associate agreement. The same provider may then disclose the same information to the same accountant under the authority of the Patient Safety Act, yet no agreement is required.

There is no apparent justification for the difference. If an agreement is appropriate under HIPAA, then it is appropriate under the Patient Safety Act. The expense is likely to be minimal because the agreements already prepared for HIPAA are likely to work here with only small changes.

VII. Proposed § 3.206(b)(10) — Disclosure to Law Enforcement

The language in this section raises substantive concerns. On page 8151, the NPRM states:

> Proposed § 3.206(b)(10) permits the disclosure of identifiable patient safety work product to law enforcement authorities, so long as the person making the disclosure believes—and that belief is reasonable under the circumstances—that the patient safety work product disclosed relates to a crime and is necessary for criminal law enforcement purposes. Under proposed § 3.208, the disclosed patient safety work product would continue to be privileged and confidential. We view this exception as permitting, for example, a disclosure by a whistleblower who would initiate the disclosure to law enforcement.

The authority for disclosure to law enforcement threatens patients. We can foresee no circumstances under which anyone should be able to disclose patient information to law enforcement under the Patient Safety Act if that information can be used in any way against a patient. If the Department is concerned about protecting whistleblowers, then it should say so specifically and narrowly. Open-ended authority can be and will be abused.

We observe that the President found it appropriate to place a procedural boundary that partially protects patients against the law enforcement disclosures allowed under the HIPAA privacy rule.

See Executive Order 13181, *To Protect The Privacy of Protected Health Information in Oversight Investigations*.[7]

We recommend strongly that disclosures to law enforcement provide express protections that prohibit the information from being used against patients who are the subject of the records. If a blanket prohibition is not acceptable, then protections that parallel Executive Order 13181 are a second choice.

Maintaining a privilege for information later down the road does not afford sufficient protection to patients because, at best, it may only prevent them from being prosecuted. It will not prevent patients from being investigated, nor will it prevent their confidential communications with their physicians from being chilled by the prospect of disclosure to the police.

As proposed, the rule leaves too much discretion on law enforcement disclosures to the PSO. The term "relates to a crime and is necessary for criminal law enforcement purposes" is exceptionally broad and can be interpreted expansively by any PSO. PSOs may in fact come under heavy pressure to turn over all their records for wide-ranging law enforcement investigations, pressure for which the PSO may not have sufficient direction in the regulation to resist.

VIII. Proposed § 3.208 — Continued Protection of Patient Safety Work Product

A. Continued Protection

On page 8153, the NPRM says that "Any person receiving such patient safety work product receives that patient safety work product pursuant to the privilege and confidentiality protections." This is fine as far as it goes. But the proposed rule does not say the same thing as the commentary.

The proposed rule says:

> Safety Work Product.
>
> (a) Except as provided in paragraph (b) of this section, patient safety work product disclosed in accordance with this subpart, or disclosed impermissibly, shall continue to be privileged and confidential.
> (b)(1) Patient safety work product disclosed for use in a criminal proceeding pursuant to section 922(c)(1)(A) of the Public Health Service Act and/or pursuant to § 3.206(b)(1) of this subpart continues to be privileged, but is no longer confidential.
> (2) Non-identifiable patient safety work product that is disclosed is no longer privileged or confidential and not subject to the regulations under this part.

[7] 65 FR 81321, December 26, 2000. < http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000_register&docid=fr26de00-124.pdf>.

> (3) Paragraph (b) of this section applies only to the specific patient safety work product disclosed.

The proposed rule is written in passive voice and imposes no clear duty on any party. It just says that the information is privileged and confidential. That is nice, but it does not say exactly what duty the recipient of the information is obliged to follow. The quoted statement from the commentary is a clearer and better statement than the proposed rule. It belongs in the rule itself.

When information goes to an entity that is not familiar with the Patient Safety Act, ignorance of the law will be almost certain. We recommend that this provision be rewritten to impose a clear duty in active voice on anyone who received the information in question in connection with a permissible activity under the Act. We also recommend that there be a duty of the party who discloses the information to label the information as subject to the Patient Safety Act and to summarize the duties that the recipient undertakes. It would be appropriate for the Department to include in the rule or in the commentary a model disclosure notice for this purpose.

The Department's decision not to require labeling is *guaranteed* to result in failure of third parties to comply with the law. There is a parallel requirement under the alcohol and drug abuse regulations in 42 CFR Part 2. Under that regulation, a strict confidentiality regime follows records. Under 2.32 of the rules, the Department required a notice to recipients for each disclosure. Even with the notice, we believe that there is much ignorance on the part of data recipients of their obligations under the alcohol and confidentiality rules. If the Department allows disclosure without any express notice under the Patient Safety Act, a high level of non-compliance with the law is certain. Patients and providers are sure to be harmed in the absence of mandated labels.

B. Hackers and Impermissible Disclosures

On page 8154, the NPRM includes this rather extraordinary statement:

> Similarly, if confidential patient safety work product is received impermissibly, such as by an unauthorized computer access (i.e., hacker), the impermissible disclosure, even when unintentional, does not terminate the confidentiality. Thus, the hacker may be subject to civil money penalty liability for impermissible disclosures of that information.

We suggest that the Department may wish to reassess this statement in light of the First Amendment's protections for freedom of speech and freedom of the press. We understand that the Department may be aiming at unauthorized computer access here. But the rule is much more broadly stated as currently written and could have wide applicability, for example, to *any* third and fourth party recipients.

If the Department wishes to reserve the right to prosecute, for example, newspapers for publishing information – and unlabelled information at that – it does so at its own peril. The Department has claimed no such authority under the HIPAA health privacy rule. In the meantime, the proposed rule appears to violate the First Amendment. We are all for privacy

protections, but they must make sense and be consistent with the Constitution. Rules that attempt to restrict the use of unlabeled information in the hands of third and fourth party recipients are neither. We wonder if there is any precedent for such a policy outside the national security environment.

If the Department wishes to include data breach provisions, it should be specific about data breaches and hacking.

IX. Enforcement

The World Privacy Forum observes that the Department proposes the same enforcement process that it adopted for the HIPAA privacy rule (page 8154). The Department has demonstrated a notable lack of civil enforcement of the privacy rule, and this is well-known throughout the health care industry.[8] It is difficult to expect that any entity will feel threatened if the Patient Safety Act receives the same degree of enforcement.

The individuals and entities that suffer the highest degree of harm from lack of enforcement are those whose confidentiality interests the Department has agreed to protect and the Department's own credibility. Tough talk about enforcement in the commentary will accomplish nothing unless the Department shows actual willingness to enforce privacy law somewhere. We wish that we could suggest a change to the proposed rule that would alleviate these concerns.

X. Conclusion and Recommendations

To reiterate our recommendations:

1. Regarding FOIA, we suggest that the rule or the commentary be revised so that it states expressly that the Secretary retains the authority other than the FOIA to determine affirmatively what information should be made available to inform the public about the operations of the Patient Safety Act, about those entities that are regulated by it, and about the Department's implementation of the Act.

2. We ask that the rule expressly mandate that all patient data be de-identified or anonymized to the greatest extent possible and at the earliest possible opportunity. Any patient data transferred by a provider to a PSO should be de-identified or anonymized unless the provider and the PSO jointly determine that identifiers are necessary.

3. Where there is justification for transferring patient data in identifiable form, the justification for retaining identifiers should be documented and retained. Further, a

[8] See Rob Stein, *Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files at Risk, Critics Say*, Washington Post, June 5, 2006. See also Peter Swire, American Progress, *Justice Department opinion undermines medical privacy*, June 7, 2005. <http://www.americanprogress.org/issues/2005/06/b743281.html>. See also Lydell C. Bridgeford, Employee Benefit News, *Health IT raises new issues for HIPAA compliance*, February 1, 2008.

review of the continuing need for identifiers should be required every three months, and there should be a presumption that any data not in active use should be de-identified or anonymized six months after transfer to the PSO.

4. PSOs that receive or create de-identified or anonymized patient data should be contractually required not to attempt to re-identify the data.

5. The proposed rule should be amended to expressly require the use of data use agreements for any data sharing. The rule must require compliance, at a minimum, with the requirements established in the HIPAA privacy rule for a data use agreement. 45 CFR 164(e)(4).

6. The NPRM should contain a requirement for the PSO to maintain an accounting of disclosures at least equal to the HIPAA privacy rule requirement. Patients must be able to use this accounting for uncovering data breaches that could lead to medical identity theft, a crime which poses significant safety risks to patients.

7. We recommend that the rule be amended to expressly provide that patients must be third party beneficiaries of all confidentiality agreements under the rule.

8. Unless the Department specifies limits on PSO disclosures directly in the HIPAA rule, there is too great a possibility that covered entities will be confused or will interpret the definition too loosely or too narrowly. The Department should amend HIPAA at the same time that it finalizes the PSO rule.

9. We strongly urge the Department to drop the words *contextually nonidentifiable (*page 8147 and following*)*.

10. We recommend strongly that disclosures to law enforcement provide express protections that prohibit the information from being used against patients who are the subject of the records. If a blanket prohibition is not acceptable, then protections should be instituted that parallel Executive Order 13181, *To Protect The Privacy of Protected Health Information in Oversight Investigations*.

11. If safety information is to be reported to the FDA or FDA-regulated entities, the reporting should not provide an opportunity for FDA-regulated entities to create, enhance, or otherwise use the information for marketing. The proposed rule should be amended to expressly prohibit any use of data for any marketing or other purpose not expressly permitted by the rule.

12. We urge the Department to require Business Associate agreements for PSOs that disclose privileged and confidential information to attorneys, accountants or other professionals for business purposes. This will bring the proposed regulation in line with HIPAA and will avoid a double standard.

13. We recommend that the provision on Safety Work Product (page 8153) to be rewritten to impose a clear duty on anyone who receives the information in question. We also recommend that there be a duty of the party that discloses the information to **label the information** as subject to the Patient Safety Act and to summarize the duties that the recipient undertakes.

14. We recommend that provisions intended to protect whistleblowers be rewritten more narrowly.

Thank you for the opportunity to comment on the proposed rulemaking.

Respectfully submitted,

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