Comments of the World Privacy Forum

To

The American Health Information Community Confidentiality, Privacy, and Security (CPS) workgroup on its Working Hypothesis

VIA email

June 4, 2007

The American Health Information Community Confidentiality, Privacy, and Security (CPS) workgroup
Office of the National Coordinator (ONC)
330 C Street, SW., Suite 4090
Washington, DC 20201

The World Privacy Forum is pleased to have this opportunity to offer comments to the American Health Information Community Confidentiality, Privacy, and Security (CPS) Workgroup in response to its May 9, 2007, Federal Register notice. The World Privacy Forum is a non-partisan, non-profit public interest research organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to health care. One recent World Privacy Forum research report, for example, discusses medical identity theft and its profound impact on patients who have been victims, as well as health care systems, both paper and electronic.

I. Introductory Comments

We begin with a general comment on activities of the Department of Health and Human Services in support of projects, standards, and policies leading toward an electronic health information network. There appears to be a fair amount of general activity, but the privacy-specific activity is lacking an overarching structure, in that privacy-related activities demonstrate scant evidence of coordination or cooperation. Specifically, the Office of the National Coordinator is undertaking a disparate array of projects such as research, standards setting, prototype building, and policy work using contractors, workgroups, state organizations, and others. Privacy comes up frequently in various contexts amongst these groups, but rarely in any effective manner, or in any way that is directed productively toward an overarching policy in concert with the other existing projects or groups. For example, AHIC is requesting comments on its "working hypothesis," but it is far from apparent whether the hypothesis has been generated solely by AHIC, or whether the hypothesis is shared with any other entities as their working hypothesis, too. We note without further comment that the National Committee on Vital and Health Statistics is covering some of this same ground.

HHS efforts on the privacy of electronic health information networks gives the unfortunate appearance of an army in retreat. Every group is moving at its own pace, in its own direction, and toward its own poorly defined objective with differing qualities of input and oversight. If there is a single, overarching organization chart and roadmap toward the future of health privacy, we have not seen it, nor have we seen any evidence of its existence. Who is going to pay attention to the workgroup's recommendations? How do they relate to other

ongoing or future activities? Who or what entity is responsible for integrating all recommendations from groups such as AHIC and NCVHS? Because of these fundamental "policy architecture" issues, we find it difficult or impossible to put the request of the workgroup in any policy context. While we recognize the fundamental difficulty of the task, we think that HHS must do better.

II. Discussion of Working Hypothesis

The workgroup's *working hypothesis* is:

> All persons and entities excluding consumers that participate in an electronic health information exchange network at a local, state, regional or nationwide level, through which individually identifiable electronic health information is stored, compiled, transmitted, or accessed, should be required to meet privacy and security criteria at least equivalent to relevant Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rate requirements.

This hypothesis reflects an assumption that the existing HIPAA privacy and security requirements are sufficient and appropriate for a networked environment. That is an assumption that the World Privacy Forum contests, and will not be alone in contesting. This is not the time or place to raise the shortcomings of the HIPAA rules for the current health care environment, but nevertheless, we note that those shortcomings are extensive. In addition, the HIPAA privacy rule is significantly unsuited for a health network environment. The rule itself reflects an

unstated assumption that most health records are maintained on paper. This is not surprising since the rule was first drafted at a time when most records were on paper. Of course, paper records are still commonplace today.

If the workgroup is proceeding on the assumption that the current HIPAA privacy rule is just fine for a yet-to-be-developed health information network, then it is wasting its own time and that of its audience. It may not be the workgroup's job to identify or fix the current problems with HIPAA, but the workgroup won't get anywhere unless it determines how an electronic environment requires changes in the current approach to privacy.

We have testified before this committee, for example, on the issue of authentication and medical identity theft. We reaffirm our previous comments on this topic to the committee, and restate here that HIPAA fails to address the problems of medical identity theft, and HIPAA fails to provide adequate (if any) remedies for victims. This is just one of many profound privacy challenges a network faces. A networked environment created without the proper controls or foresight can exacerbate these, and other, problems mightily.

Returning to the language of the hypothesis, we question the phrase "excluding consumers." We cannot judge whether a consumer exclusion is appropriate without more explanation. Are consumers who use the network as patients (or, to use the HIPAA language, *individuals*) to be exempt from any requirements for authentication? We recognize that a consumer accessing the health network will have different status than a health care provider, but that does not mean that the consumer should be exempt from meeting some obligations or complying with network rules.

III. Enforceable Mechanisms

The workgroup's interest in finding appropriate, effective, and feasible ways to enforce confidentiality, privacy, and security protections is welcome. It is appropriate and welcome that the workgroup is looking for enforcement guidance outside the Department, and we encourage the workgroup to continue its efforts in this area, which could be productive. HHS has not demonstrated much interest in enforcing existing privacy rules to date, and the lack of intensity and effectiveness in enforcement only serves to underscore the importance of better enforcement mechanisms for any health information network.

A health information network will require multiple and overlapping enforcement mechanisms. We limit our current comments to one basic concept. ***Any health information network should provide expressly that the purpose of privacy rules is to protect individuals and that individuals are intended third-party beneficiaries of the agreements.*** The goal is to make it easier for individuals to pursue remedies against those who misuse data or undermine the privacy or other interests of the subjects of health records. In the HIPAA health privacy rule, the Department left the third-party beneficiary issue unresolved. That was a mistake.

The workgroup must recognize that the privacy stakes in a health information network are much greater than for a paper-based health record system. Existing HIPAA enforcement mechanisms for privacy are a failure to date. If individuals find any remedies for breach of health privacy today, they come under state law. A third party beneficiary rule would make existing remedies easier to use. Resolving this issue is one element of an enforcement strategy, but it is not the only one. It is just the one we chose to emphasize in these comments.

IV. Relevant Requirements

The inquiry about whether particular HIPAA rules should apply or not apply to all parties involved in a health information network is both intriguing and premature. While we understand why AHIC is asking this question, we also recognize that the question is out of sequence -- it is far too detailed a question to ask at this time when virtually nothing about the network or the structure of privacy regulation is known. Until someone has made a determination about who will have direct access to the information in a health network, it is impossible to address the application of privacy rules to particular players. We also refer you to the previous brief discussion about the shortcoming of the existing HIPAA privacy rule.

Currently, the HIPAA privacy rule identifies a large number of institutions (in addition to health care providers and insurers) that have the ability to obtain health information without the consent of the data subject. These include public health agencies, researchers, courts, coroners, funeral directors, law enforcement, national security, fraud investigators, litigants, and many more. None of these institutions is subject to the HIPAA privacy rule (unless they happen to also be serving as health care providers or insurers). Will these unregulated secondary users of health records have direct access to a health information network? Until we know who or what entities will have the ability to retrieve records from a health information network and in what amounts under what circumstances, it is impossible to address the question of what rules should or should not apply.

An alternative policy would require that health privacy rules follow records as those records are transferred to the hands of secondary users. Rather than apply privacy rules only to

direct network users, those entitled to obtain health records could be obliged to follow privacy rules whether or not they obtained records directly from the network or only from the more limited class of authorized network users. This could be what the workgroup contemplates, and we in fact suggest this.

While suggesting this, we recognize that this approach – that although useful -- is rarely found in American privacy law outside of the substance abuse confidentiality rules in 42 CFR Part 2. If the workgroup contemplates such a significant new approach to privacy policy, it should say so directly. It would require a set of privacy rules with greater applicability and complexity than HIPAA, probably by an order of magnitude.

With this suggestion, we end up where we started with this inquiry. Until we know more about the network and type of privacy regulation expected, it is impossible or pointless to discuss the possible applicability or non-applicability of an unknown privacy regime to an unidentified group of health information users. We reiterate that the workgroup should conduct its inquiries at a higher level of abstraction first.

V. Business Associates

It is the question about business associates that gave rise to the thought that the workgroup contemplates a privacy rule applicable to all secondary users in possession of health data. The question seeking factual information about the regulation of business associates could produce interesting information, but we doubt it will help much. We have three thoughts to offer.

First, many business associates of covered entities also provide support services to organizations in other industries. Those other industries may have their own legislative, regulatory, or other standards for ensuring that data remains secure and private while being processed by business associates. A question for business associates is how they would address processing personal data for different clients under different privacy, security, and enforcement regimes. It would also be interesting to know whether such a possibility is actually much different from the requirements that they face today in the marketplace and have faced for some time.

Second, the inquiry is likely to show that business associates prefer the regime with the least likelihood for actual enforcement and with the smallest penalties. At present, the absence of actual enforcement of the privacy rule against covered entities or business associates makes a choice irrelevant. Choosing between flogging with a wet noodle and flogging with a wool thread may be a difficult choice, but the answer does not matter much. A finding that business associates prefer more procedural uniformity and the least possible enforcement will not likely tell the workgroup anything of interest.

Third, the business associate inquiry is too narrow. Any question about the proper scope of direct privacy regulation cannot be resolved by asking about business associates only. The large number of secondary users who are neither business associates nor covered entities calls for a broader look at the question of the scope of privacy regulation for a networked environment.

VI. General Questions

We find it disconcerting that the workgroup's first concern about divergent privacy regimes is the effect on competitiveness. Preserving competitiveness is not our first concern about privacy regulation. Indeed, it does not appear anywhere on our list of privacy concerns.

We would have hoped that a workgroup focused on privacy would be asking about the effect of divergent privacy regimes on *consumers* first. We are at a loss to understand why the workgroup is not asking about the ethical and moral obligations of health care providers to protect patient privacy regardless of the competitive consequences vis-à-vis potentially unregulated data brokers. We cannot understand why the workgroup is not interested in informing patients who agree to the transfer of their personal health information to unregulated commercial PHR companies that their actions put all of that information at risk for commercial exploitation.

The question seems to suggest a potential "race to the bottom," where no record keeper is required to comply with privacy rules in order to preserve its ability to "compete" with some other actual or theoretical organization that is not regulated. We hope that our inference here is wrong, but we remain concerned that the workgroup's eyes are focused in the wrong direction.

VII. Conclusion

We respect the workgroup's request for input regarding these matters, and appreciate the opportunity to participate in this dialog.

Respectfully submitted,

Pam Dixon
World Privacy Forum
760-436-2489
http://www.worldprivacyforum.org