

June 12, 2007

The Honorable Michael O. Leavitt

Chairman

American Health Information Community

200 Independence Avenue, S.W.

Washington, D.C. 20201

Dear Mr. Chairman:

The American Health Information Community (AHIC) has identified and prioritized several health information technology applications, or “breakthroughs,” that could produce specific and tangible value to health care consumers. To address these breakthrough areas, the Confidentiality, Privacy, and Security Workgroup (the CPS Workgroup) was formed and given the following broad and specific charges:

Broad Charge for the Workgroup: Make recommendations to the AHIC regarding the protection of personal health information in order to secure trust, and support appropriate electronic health information exchange.

Specific Charge for the Workgroup: Make actionable confidentiality, privacy, and security recommendations to the AHIC on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs.

INTRODUCTION:

The CPS Workgroup issues the following recommendation as a significant step in our analysis to determine what, if any, additional protections beyond those currently provided are needed to ensure the confidentiality, privacy, and security of individually identifiable health information in an electronic health information exchange environment. This letter provides context for the AHIC as it considers issuing the recommendation to the Department of Health and Human Services (HHS).

Recommendation:

All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be

required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA [FN1] requirements (45 CFR Parts 160 and 164).

Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a Business Associate Agreement as provided for in HIPAA).

As the prevalence of electronic health information exchange increases, it is clear that the amount of readily available health information and access to it will also increase. The recommendation above began as a “working hypothesis” a consensus-based approach used by the CPS Workgroup to prove or disprove a concept through public testimony and CPS Workgroup deliberation.

Through several meetings, the CPS Workgroup heard testimony from a variety of stakeholders in an effort to better understand the impact persons and entities in an electronic health information exchange environment could have on the current health privacy and security regulatory structure. Many of the testifiers who spoke to the Workgroup were considered to be “non-Covered Entities” under the Health Insurance Portability and Accountability Act (HIPAA). All of them attested to voluntarily complying with the requirements of the HIPAA Privacy and Security Rules (the Rules) in whole or in part in order to conduct business and ensure consumers that health information would be protected. When asked if being covered under the Rules or something equivalent would negatively impact their business, many believed the impact would be negligible, because they were already meeting or exceeding the requirements of the Rules.

Based on this testimony and the other information gathered by the CPS Workgroup, we are recommending that there be a minimum set of standards a baseline for participation in an electronic health information exchange network, regardless of a participant’s “status” under the Rules. The CPS Workgroup believes our recommendation represents an important step in assessing the obligations that are appropriate for persons and entities participating in such a network that have responsibility for such valuable personal information.

The recommendation above uses the Rules as an initial measure of comparison because the Rules establish a national baseline from which to start our analysis. Our recommendation is not a critique of the Rules, but rather a platform from which the CPS Workgroup can evaluate if, in the future, the overall baseline standard for participating in these networks should be changed to a standard that is different from or exceeds the current Rules. We will be addressing issues related to this baseline in the near future. Additionally, our recommendation is not intended to interfere with or contradict more stringent state laws that pertain to the confidentiality, privacy, and security of health information.

Moreover, as a corollary to our recommendation (particularly the idea that participating entities should be required to meet the “relevant” requirements of HIPAA as a baseline standard), we plan to further refine our position through future meetings (described below in “next steps”). We will determine what, if any, regulatory or practical differences may (e.g., gaps or non-applicable requirements) exist for certain categories of participants and evaluate whether there are specific requirements of the Rules that are not directly applicable to certain entities (e.g., a privacy notice requirement for persons or entities that have no direct relationship with consumers).

RATIONALE:

“Participate Directly”

The CPS Workgroup believes it is important to distinguish between persons and entities that “participate directly” or are “direct participants” in an electronic health information exchange network, and persons and entities whose participation is indirect or tangential.

Persons or entities that “directly” participate in an electronic health information exchange network would include the network itself (or the entity/organization that runs it) and those who engage in and connect to the network for a specified purpose to store, compile, transmit, modify or access health information from the network. “Indirect participants” contract with “directly participating” persons or entities and receive health information, without accessing the network themselves, but from these “direct participants” solely for the purposes of serving a legitimate business need of the “direct participant.”

We offer for illustration the example of a large physician group practice that interacts with its patients and with other providers via a regional health information organization (RHIO). The group practice and the RHIO would be considered direct participants in the electronic health information exchange network. But if the group practice hires an audit firm to conduct an analysis of all the claims it submitted through the network over the past three months for compliance with proper billing practices, the audit firm whose relationship to the electronic health information exchange network is solely via contract or arrangement with the group practice would not be considered a direct participant in the exchange.

The Business Associate Model

The CPS Workgroup addressed as part of our recommendation a concern that we have with the role Business Associates will play in an electronic health information exchange environment. Under the current regulatory framework there are persons and entities (Covered Entities) directly accountable to HHS for failure to comply with the Rules, and Business Associates who are only accountable to the terms in their contract with a Covered Entity. But in this new electronic environment, some entities who currently qualify as Business Associates are responsible for, and directly involved in similar, if not more, activities related to health care information than HIPAA Covered Entities. It is the

CPS Workgroup's belief that it is not in the public's best interest to hold these entities to different accountability or enforcement standards than Covered Entities.

In accordance with the first part of our recommendation, the CPS Workgroup believes that any person or entity whose particular role in an electronic health information exchange network would make them a "direct participant," should be held directly accountable for its actions in a manner similar to those who are Covered Entities under HIPAA (i.e., this accountability is independent of any contractual requirements they may have to follow). Thus, the CPS Workgroup does not believe that Business Associate Agreements (contracts) will hold these types of Business Associates to a standard level of accountability and ensure they adequately protect health information the way a Covered Entity must under HIPAA. While we have not at this time prescribed a method to implement the recommendation above (meaning that we have not reviewed the question of whether this recommendation should be implemented by a new law, a revised HIPAA regulation, a new regulation or through some other means), we believe that these protections should be enforced uniformly across all "direct participants" (i.e., "direct participants" are subject to one set of rules that are enforced independent of contractual or other agreements). Our recommendation is that the same standards be applied meaning that if some "direct participants" face potential civil or criminal sanctions, then all "direct participants" should face these sanctions.

Although the first part of our recommendation was agreed to without objection, one member of the CPS Workgroup did not share the opinion of the majority and requested that this view be noted for the record the obligation of a Business Associate to comply with any confidentiality, privacy, and security requirements should be enforced through its Business Associate Agreement with the person or entity that directly participates in the network.

NEXT STEPS:

The CPS Workgroup considers this recommendation to be one of many confidentiality, privacy and security issues we will present for AHIC deliberation. Over the next several months our approach will consist of research and public comment and testimony to evaluate, at a more granular level, two key questions raised by the recommendation above.

First, we will examine what constitutes a "relevant" HIPAA requirement for particular "direct participants" in the network. Our current approach is to assume that all of the Rules' requirements apply to everyone who "directly participates" in electronic health information exchange networks. However, given that the Rules were written to be applicable to Health Plans, Healthcare Clearinghouses, and Health Care Providers conducting electronic healthcare transactions, we understand that some persons or entities may have an appropriate reason for not needing to meet a particular requirement. In our May 9, 2007 Federal Register meeting notice, we posed questions for the public in order to gain more insight into this issue. We plan to begin our discussion at our next meeting.

Second, we will analyze what, if any, additional confidentiality, privacy, security protections may be needed beyond those already contained in the Rules in order to ensure trust in an electronic health information exchange environment. Specifically, we will be addressing whether there are important differences in the operation of health information exchange networks that require a baseline standard that is more stringent than the Rules.

These recommendations are supported by information obtained through research and testimony to the Confidentiality, Privacy, and Security Workgroup, which is contained in the supporting documents available at <http://www.hhs.gov/healthit/ahic>.

Thank you for giving us the opportunity to submit this recommendation. We look forward to discussing this recommendation with you and the members of the American Health Information Community.

Sincerely yours,

Kirk J. Nahra

Chair

Confidentiality, Privacy, and Security Workgroup

FN1 Health Insurance Portability and Accountability Act of 1996