

February 26, 2008

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 CPS 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 CPS 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.

Background:

On June 12th, 2007, the AHIC accepted the following for recommendation to the Secretary of the Department of Health and Human Services.

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 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).

In our June recommendation letter, the CPS Workgroup set forth two areas for additional inquiry. We expressed our intent to first examine what constitutes a “relevant” HIPAA requirement for particular “direct participants” in an electronic health information exchange network, as that term is defined in the June letter. After determining relevancy we noted that we would focus on what, if any, additional confidentiality, privacy, and security protections may be needed beyond those already contained in the HIPAA Privacy and Security Rules (the Rules) in order to raise public trust in an electronic health information exchange environment. The recommendations in this letter focus solely on the first question: whether all requirements under the Rules are relevant to all entities who are direct participants in an electronic health information exchange network but who are not currently covered by the Rules.

Based on public testimony and CPS Workgroup analysis and discussion, the CPS Workgroup recommends that all persons and entities (excluding consumers) that participate directly in or comprise an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to the Rules, except as expressly set forth in this letter. To further clarify, with the exception of the recommendations below which provide specific exemptions we recommend that all of the Rules requirements apply and are relevant to other non-Covered Entities such as those offering PHRs. Our recommendations specifically pertain to health information exchanges (HIEs) and regional health information organizations (RHIOs) (collectively referred to in this letter as HIEs) that do not have “independent relationships” with patients or consumers and in our view should not be required to meet: (1) §164.520 Notice of privacy practices for protected health information; (2) §164.522 Rights to request privacy protection for protected health information; (3) §164.524 Access of individuals to protected health information; (4) §164.526 Amendment of protected health information; and (5) §164.528 Accounting of disclosures of protected health information.

The particular HIPAA Privacy Rule requirements cited above directly implicate, and are dependent on, a consumer or patient’s relationship with a health care provider or health plan that is a HIPAA Covered Entity. Based on our research to date, few, if any, HIEs currently in operation or contemplated have, or will have, independent relationships with individual patients or consumers. To further clarify, we would consider an HIE that uses or discloses health information directly to, or on behalf of, a patient or consumer rather than other participants in the HIE as having an independent relationship with that patient or consumer. For example, an HIE that offers PHRs to patients or consumers would have an independent relationship, and consequently, would be expected to follow all of the HIPAA Privacy Rule requirements. Today, by contrast, HIEs typically operate as intermediaries to move health information to and from persons and entities including Covered Entities such as health care providers. Rarely will a consumer or patient be called upon to provide information directly to or request information directly from an HIE, but they will continue to do so through their health care provider, health plan, or PHR service provider with whom an independent relationship exists.

Because we have already recommended that those persons and entities who participate directly in an electronic health information exchange network should meet requirements

equivalent to these particular HIPAA rules, and HIE access to health information will be solely as an agent or Business Associate of those persons and entities, there is no need to also impose these requirements on HIEs. In fact, we have concerns that in some situations, it may be counter-productive or inappropriate for an HIE that does not have an independent relationship with the consumer or patient to have direct responsibilities for fulfilling these individual rights. But this is a rapidly evolving environment, and as explained in more detail below, if HIEs establish independent relationships with patients or consumers, the Rules should apply equally to those entities as they do to other Covered Entities.

It is important to note that the recommendations below are neither meant to discount or detract from the privacy rights of patients or consumers, nor reduce the type of protections that should be provided in an electronic health information exchange network. Our recommendations are meant to pragmatically exempt particular entities (HIEs) from directly providing certain HIPAA Privacy Rule requirements to patients or consumers in situations where they are acting on behalf of another entity that is participating in the HIE. All rights will continue to apply in full through the entity with whom the consumer or patient has an independent relationship. Moreover, HIEs will continue as they do today to assist these Covered Entities as appropriate in providing individual rights pursuant to existing Business Associate Agreements.

Recommendations:

Notice of Privacy Practices

Recommendation 1.0: The CPS Workgroup recommends that the HIPAA Privacy Rule requirement to provide a notice of privacy practices to consumers is not relevant to HIEs that do not have an independent relationship with consumers or patients. Therefore, we recommend that HIEs be exempted from this specific HIPAA Privacy Rule requirement.

Recommendation 1.1: The CPS Workgroup recommends that HIEs make publicly available on their website (or through other means) a document that reasonably and accurately describes how they use and disclose health information and their privacy policies and practices, as well as how they safeguard patient or consumer information.

The exemption of a notice requirement does not mean that HIEs can use or disclose health information in a way that a Covered Entity or Business Associate could not. Rather, it means they do not have to disseminate a notice to a patient or consumer the way a health care provider or health plan must. If, in the future, HIEs were to establish independent relationships with individuals, the CPS Workgroup would consider this requirement to be relevant to such entities and expect an HIE to provide a notice equivalent to the one required under the HIPAA Privacy Rule today.

Individual Rights

Recommendation 2.0: The obligation to provide the individual rights below should remain with the current Covered Entity who today has the independent relationship with the patient or consumer and not the HIE.

Testimony has suggested that many HIEs today exchange health information for a limited set of purposes under a limited set of conditions and operate in most instances without any patient or consumer interaction (i.e. a “non-independent relationship”). However, if, in the future, an HIE were to establish independent relationships with individuals, the CPS Workgroup would consider this requirement to be relevant to such entities and expect the HIE to provide individuals rights equivalent to those required under the HIPAA Privacy Rule today. While we recommend that the responsibility for fulfilling these individual rights continue to rest with the person or entity that has an independent relationship, we do not intend this recommendation to disrupt or alter in any way the obligations of an HIE to assist in performing these rights consistent with their obligations under existing Business Associate Agreements.

Recommendation 2.1: We recommend that HIEs that do not have independent relationships with patients or consumers be exempted from the obligation to provide them with direct access rights.

Recommendation 2.2: We recommend that HIEs that do not have independent relationships with patients or consumers be exempted from the obligation to provide them with restriction or confidential communication rights.

Recommendation 2.3: We recommend that HIEs that do not have independent relationships with patients or consumers be exempted from the obligation to provide them with amendment rights.

Recommendation 2.4: We recommend that HIEs that do not have independent relationships with patients or consumers be exempted from the obligation to provide them with an accounting of disclosures.

We believe that the individual rights mentioned above are best provided by the persons and entities that have independent relationships with individuals. HIEs would still have an obligation consistent with any existing Business Associate Agreements to assist a Covered Entity in providing these individual rights where appropriate. For example, to assist a Covered Entity in responding to an amendment where appropriate (i.e., satisfying the “informing others” requirement within §164.526(c)(3)).

Next Steps:

As mentioned above, having completed the task of determining relevancy, we will next turn to the issue of what, if any, additional confidentiality, privacy, security protections should apply to persons and entities that participate directly in electronic exchange of health information beyond those already contained in the Rules to raise public trust in an electronic health information exchange environment. Specifically, we will be addressing

whether there are important differences in this environment for HIEs and PHRs and whether those differences require standards that are 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 these recommendations. We look forward to discussing this recommendation with you and the members of the American Health Information Community.

Sincerely yours,

Kirk J. Nahra
Co-Chair
Confidentiality, Privacy, and Security
Workgroup

Deven McGraw
Co-Chair
Confidentiality, Privacy, and Security
Workgroup