September 28, 2009

The Honorable Kathleen Sebelius
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Madam Secretary:

Re: Protection of the Privacy and Security of Individual Health Information in Personal Health Records

The National Committee on Vital and Health Statistics (NCVHS) is the Department of Health and Human Service's statutory public advisory body on health data, statistics, and national health information policy. The NCVHS has historically made recommendations about health information privacy, confidentiality, and security, and has responsibility under federal law for making recommendations to HHS on the Health Insurance Portability and Accountability Act (HIPAA).

Personal health records (PHRs), a growing part of the health information landscape, can provide substantial benefits (such as continuity of care and patient safety) for patients, caregivers, health care providers, and society more generally. However, PHRs also raise important privacy, confidentiality, and security concerns. Due to these concerns, the American Recovery and Reinvestment Act (ARRA) requires a report to be prepared by HHS, in consultation with the Federal Trade Commission (FTC)identifying privacy and security requirements for PHRs that are not operated by HIPAA covered entities.[1] This letter contains recommendations about the privacy and security of PHRs for you to consider when creating this report, or considering other policy changes.

A PHR is an electronic record of "individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual."[2] PHRs are distinguished from electronic health

[1] ARRA, §13424(b)(1) (2009).
[2] ARRA § 13400(11).

records (EHRs) in that the latter are "created, gathered, managed, and consulted by authorized health care clinicians and staff."[3]

PHRs take many different forms and are rapidly evolving. In some cases, the PHR is a "portal" view into one or more providers' EHRs. In other cases, the PHR is created and operated by a third party which is not regulated or subject to HIPAA protection. PHRs may be managed by consumers, who may include patients themselves, their caregivers, or their appropriately designated personal representatives. Despite the important benefits of PHRs, consumers might not fully understand the extent to which their information is protected by law and, consequently, may inadvertently consent (e.g., through an "I Agree" button) to unintended information sharing and use.

PRIOR NCVHS ACTIVITIES REGARDING PHRs

Over the past few years, NCVHS has made a number of recommendations about PHRs specifically and about the privacy and security of individual health information more generally. Most importantly, NCVHS has recommended that common privacy and confidentiality rules apply to all entities that collect, retain, use, compile, or disclose identifiable health information, under a comprehensive federal privacy law.[4]

In February 2006, NCVHS issued a report making general recommendations on PHRs.[5] In that report, the Committee noted that PHR systems were evolving rapidly and served a variety of beneficial functions for consumers and their caregivers, healthcare providers, payers, employers, and society more generally. NCVHS recommended developing a framework for characterizing PHRs and educating consumers based on that framework. NCVHS also recommended developing privacy best practices for PHRs and a model notice of privacy practices in a form that consumers could easily understand. For the many PHRs that are not within the scope of the privacy and security protections afforded by regulations under HIPAA, NCVHS recommended voluntary adoption of strict privacy practices and a policy of non-disclosure of information without consumer authorization. Since that report, PHRs have continued to evolve, but guidance regarding privacy best practices has been limited. For example, in December 2008 HHS published a set of privacy principles for health information technology and a model privacy notice for PHRs for comment.[6] But, to date, a final model notice has not been provided.

In today's market, there are many forms of PHRs. Some PHRs are portals maintained by health care providers, through which consumers may view their EHRs. In

---

[3] ARRA § 13400(5).

[4] NCVHS, *Privacy Report to the Secretary: Recommendations on Privacy and Confidentiality*, 2006-2008, http://ncvhs.hhs.gov/privacyreport0608.pdf.

[5] NCVHS, *Personal Health Records and Personal Health Record Systems* (2006) <http://ncvhs.hhs.gov/reptrecs.htm>

[6] HHS, *Draft Model Personal Health Record (PHR) Privacy Notice* (Dec. 2008), http://healthit.hhs.gov/portal/server.pt?open=512&objID=1176&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true

some provider-maintained PHRs, consumers may only view information as entered by their health care provider. In other provider-maintained PHRs, consumers are able to enter their own information—for example, blood pressure readings taken at home, and depending on the PHR design, the provider may or may not be able to access such consumer-entered information. Other PHRs have the ability to download information from EHRs maintained by the patients' health care providers or health plans, as well as to incorporate information entered by the consumers. Still other PHRs are composed solely of information entered by the consumer, for the consumer's own use. In some forms of PHRs, consumers may also enter information for purposes extending beyond their own use, such as sharing their information with others who have similar medical conditions, or allowing their information to be used for research. The recommendations in this letter are intended to apply only to PHR systems and not EHR systems maintained by a health care provider or claims systems maintained by a health plan, even if the information from such systems can be viewed by consumers through a PHR portal.

Understanding the application of the HIPAA Privacy Rule and its limitations is critical to understanding the current state of privacy protection for PHRs. There are limits to the protections provided by the Privacy Rule, but consumers may not understand these limits nor their significance for information patients enter into PHRs themselves. For example, the Privacy Rule does not protect information from certain disclosures for law enforcement purposes,[7] but consumers may assume their PHR information is completely private. Furthermore, only PHRs that are created or managed by HIPAA covered entities (or business associates of covered entities) must comply with the Privacy Rule. Consumers may believe that information they enter into any PHR receives HIPAA privacy protection, whether or not the PHR supplier is covered by HIPAA. Moreover, once information is transferred from a covered entity to a PHR supplier that is not covered by HIPAA, a consumer may not realize that protections afforded under the Privacy Rule will no longer apply. The differentiation between "tethered" PHRs (those that are integrated with a HIPAA covered entity's clinical or claims systems) and "untethered" PHRs (PHRs that are not integrated with a covered entity's systems) is becoming less clear, as PHRs are increasingly aggregating information from multiple sources (including providers, payers, pharmacies and consumers themselves). As a result, concerns have been voiced about the adequacy of privacy and security protections for PHRs, whether or not they are covered by HIPAA.

In order to develop additional recommendations regarding privacy and security of information in PHRs, the Privacy, Confidentiality and Security Subcommittee of NCVHS held hearings on May 20-21, 2009, and on June 9, 2009. The hearings included testimony from experts about how PHRs specifically, and health information technology generally, are expected to evolve. The Subcommittee also heard testimony from vendors of free-standing PHRs, and from representatives of PHRs offered by health care providers and payers. Consumer advocates and experts on the privacy and security of health information testified, as did representatives of the two Centers for Medicare and

[7] 45 C.F.R. § 164.512(f) (2009).

Medicaid Services (CMS) PHR demonstration projects (in South Carolina and in Utah/Arizona).

POLICY THEMES

Four important themes emerged from the hearings: (1) the need for a standard set of fair information practices to govern consumer rights across all PHRs, (2) the need to maintain regulatory flexibility to foster development and innovation in the field of PHRs, (3) the importance of protecting consumers from unanticipated or inappropriate uses or disclosures of health information in their PHRs, and (4) the need to develop a consumer education strategy that will ensure appropriate understanding of the purposes, uses, and privacy and confidentiality limitations of PHRs. To address these themes, it is vital that there be true informed consumer consent, including to any disclosure of information in PHRs. Such informed consent requires absolute transparency into a PHR supplier's privacy and security practices, as well as effective education and understanding on the part of consumers.

NCVHS,[8] the Office of the National Coordinator for Health Information Technology (ONC),[9] and the Markle Foundation,[10] among others, have separately recommended sets of fair information practices that include consent and transparency regarding information collection, and permissible information uses and disclosures. These information practices require that, as PHRs are maintained for the benefit of consumers, information in PHRs must be adequately secured and not be collected, used, or disclosed without truly informed consumer consent.

Fair information practices discussed at the hearings also include:

- Consumers should be able to receive electronic copies of information contained in a PHR.
- Consumers should be able to make corrections to information they have entered into their PHRs or others such as family members have entered on their behalf.
- Consumers should be able to exercise control of disclosures at a level of granularity that permits them to protect sensitive information or information they have entered themselves into their PHR.

---

[8] NCVHS, *Privacy Report to the Secretary: Recommendations on Privacy and Confidentiality*, 2006-2008, http://ncvhs.hhs.gov/privacyreport0608.pdf.

[9] ONC, *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information*, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

[10] Markle Foundation, *Connecting Consumers: Common Framework for Networked Personal Health Information*, http://www.connectingforhealth.org/phti/reports/overview.html

- Substantive changes in use or disclosure policies should require proactive communication to the consumer of such changes and a prospective explicit renewal of consumer consent.
- Information security, quality, integrity and availability should be maintained through the use of appropriate administrative, technical, and physical safeguards.
- The consumer should have the right to an accounting of who accessed the consumer's information, as well as a process to address consumer complaints.
- PHR suppliers should be required to take appropriate steps to mitigate a security breach or inappropriate use or disclosure (including providing timely notice to consumers of any privacy or security breaches that may have occurred).

Finally, certain disclosures or uses of the information in PHRs are likely to be particularly troubling to consumers. Many consumers may object to use of their PHR information for marketing purposes. Some types of health information may be especially sensitive or likely to give rise to stigmatization or discrimination, and as a result, disclosures to insurers or to employers may appear risky to consumers who fear the loss of benefits or a job. In addition, many consumers object to their information (either individually or as part of a database) being sold without their consent. These uses and disclosures should be specifically identified for consumers and should require explicit consent at the time that the disclosure from the PHR is contemplated.

ADDRESSING THE NEED FOR TRANSPARENCY REQUIREMENTS AND INFORMED CONSENT WITH RESPECT TO PRIVACY PRACTICES

If consent is to be fully informed, information collection practices, planned information uses, and any information disclosures must be fully transparent to consumers.

Unfortunately, there are numerous reasons why transparency is difficult, including:

- Computer literacy varies, and some consumers may have limited familiarity with interactive web technologies common in PHRs.
- At the point of initiation of a PHR, consumers may "click through" privacy notices and consents without fully reading or understanding them.
- Consumers may not be aware that protections afforded to information in one context do not follow information transferred to another context. Consumers may assume erroneously that privacy protections that apply to an EHR carry forward when information is transferred outside of the EHR to a PHR. Consumers also may not be aware that the information consents or restrictions that they make in one PHR do not carry forward if information is transferred to another PHR.
- PHR suppliers typically reserve the right to change the PHR's terms and conditions, including the privacy terms. Consumers who may have invested

considerable effort in creating a PHR may find it difficult to change PHR suppliers even if changes in terms are unacceptable to them.

- Consumers may not be aware of their rights or the disposition of their information in the event that the PHR supplier is sold, merges with another entity, or goes bankrupt.
- Consumers may not realize that following a link to a site outside of the PHR may reveal their identity or information about them.
- Consumers may not be aware that health information (even without explicit identifiers) may be re-identified using information from other publically available sources.

At 12 pages long, the "Draft Model Personal Health Record (PHR) Privacy Notice" that was published by HHS illustrates the difficulty in providing information that is clear, complete, and also concise. Presenters at the hearings emphasized a variety of problems in relying on this or a similar notice as a basis for ensuring transparency (5/20 Marshall).

RECOMMENDATIONS

NCVHS heard consistently during the hearings that many different constituencies believe it is critically important to develop a clear set of common privacy and security standards for all PHRs that consumers will be able to understand and to rely on with respect to the information in their PHRs.

I. Transparency and Informed Consent to Information Uses and Disclosures

Recommendation I.A. *Consumers should have the right to consent or to withhold consent to uses and disclosures of their information by a PHR supplier. This recommendation does not apply to information in EHRs maintained by health care providers.*

The need for consumer consent was a consistent theme across the hearings. PHRs should not be structured in a manner that results in disclosure of health information without the consumer agreeing to the disclosure. For example, it would be inappropriate for a PHR website to contain advertising or other links that reveal the consumer's health information—without the consumer's explicit consent to the disclosure.

However, a consumer's ability to control access to information in a PHR, if tethered to an EHR, should not be allowed to affect the integrity of the EHR. Ensuring the integrity of information in a health care provider's EHR is critical to ensuring quality in patient care. It may not be easy to differentiate between health care provider-supplied and consumer-supplied information, because of the multiple forms of tethered and un-tethered PHRs on the market today. Therefore, the key criterion regarding whether information becomes a part of an EHR is not the source of the information, but whether it is incorporated into the record relied on by the provider in making treatment decisions. If a tethered PHR is designed to integrate consumer-provided information into the EHR, then this feature should be made clear to consumers before they enter any information.

The principle of consumer consent governs information that a patient authorizes to be transferred into a PHR, including information downloaded from EHRs or from claims systems.

Recommendation I.B. *The process of consent to uses and disclosures of consumer information contained within a PHR, and to other PHR supplier practices, should be structured in a manner that enhances consumer understanding.*

NCVHS heard considerable testimony that "click through" processes, while common, do not effectively inform consumers regarding anticipated practices of the PHR supplier, or uses and disclosures of their information. Consumers may be eager to complete their planned transactions (sometimes not even knowing what the software application does) and simply click "I agree" to the online terms. NCVHS also heard testimony that the ONC draft notice of privacy practices, in its current form, does not yet succeed at conveying information in a way that is likely to be useful to consumers.

Recommendation I.C. *Consumers should be informed that information transfers from HIPAA-covered entities or their business associates to PHR suppliers not covered by HIPAA will place their health information outside the scope of HIPAA (though some protections may still be afforded through FTC regulations).*

The HIPAA notice of privacy practices given to consumers by providers, health plans and other covered entities has become familiar to consumers. Some PHRs are offered by entities that are covered by HIPAA or that have business associate agreements with HIPAA covered entities—PHRs offered by health insurers, or by employers in connection with health plans, for example—and consumers may think of these as just an extension of their health records. Consumers may also authorize transfer of their protected health information from health care providers to PHRs offered by entities that are not within the scope of HIPAA, making the health information lose its 'protected' status under HIPAA. Before consumers authorize transfer of their HIPAA-protected information to a non-covered PHR, they should be warned explicitly that HIPAA will no longer apply, though FTC regulations may still apply.

Recommendation I.D. *Changes in PHR terms, policies, and procedures governing practices, uses and disclosures should not be permitted without explicit notice to consumers and prospective explicit consumer consent (i.e., a PHR supplier should not be able to obligate a consumer simply by posting revised terms on its website). Consumers should be given a reasonable period of time within which to decide whether to agree to the change, arrange for the transfer of their information, or request deletion of their information.*

Several witnesses testified that many PHR suppliers reserve the right to change their terms simply by posting the revised terms on their website. The NCVHS believes that this practice is not adequate as a method for obtaining consumer consent. Some witnesses pointed out that consumers may have invested considerable time and effort in

the development of their PHRs, and as a result, it might be difficult for them to change to a different PHR supplier should a change in terms be unacceptable to them.

II. Other Fair Information Practices

Recommendation II.A. *Consumers should have the right to an electronic copy of the information in their PHR in a format that allows it to be transferred directly to, or reentered in, a different PHR.*

Recommendation II.B. *The Secretary should encourage PHR suppliers to develop their products in a manner that facilitates interoperability by incorporating national standards for exchange of information. If any PHR certification processes are developed, they should incorporate national standards for exchange of information.*

A consumer may invest considerable time establishing a PHR. Without the ability to electronically transfer information in a standard format, it may be impossible for the consumer to switch to a different PHR. As a result, if a PHR supplier changes privacy practices in a manner that is unacceptable to the consumer, the consumer's only effective choices may be either to remain with the supplier or to delete the consumer's entire PHR record. Thus, portability of PHR information is important to giving the consumer the ability to select PHR suppliers that the meet privacy, confidentiality, and security expectations that are acceptable to the consumer.

Recommendation II.C. *Consumers should have the ability to add, correct or delete information they have entered into their PHRs; this does not imply that a consumer has the right to change directly information in a health care provider-maintained EHR. Rather, the consumer should follow the process set out under the HIPAA Privacy Rule to request the correction of information in an EHR.*

When the consumer authorizes information to be added to a PHR, the consumer should be able to control that information. But, this does not imply that a consumer should have the right to change information in a health care provider-maintained EHR, even if it includes information that was entered by the consumer through a PHR. (A consumer does have the right under HIPAA to request correction of information in an EHR.[11]) If a PHR receives information from an EHR, and the EHR source is later updated, the PHR should be updated by following the process described in the HIPAA Privacy Rule.

Recommendation II.D. *Consumers should have the right to request that all of the information in their PHR be deleted, whatever the source of the information.*

Consumers may find that they no longer agree with the privacy and security practices of their PHR suppliers, or may decide for other reasons that they no longer wish to have PHRs maintained on their behalf. Consumers should understand, however, that a

[11] 45 C.F.R. § 164.526 (2009).

decision to delete information in a PHR does not affect the status of information in an EHR maintained by a health care provider, nor other places where the information has been transferred.

Recommendation II.E. *Consumers should have the right to an accounting of the uses and disclosures of their information.*

Many presenters at the hearings emphasized the importance of tracking uses and disclosures to consumer trust in PHRs. Consumers may wish to know who has accessed their information as a way to ensure accountability or to facilitate correction of errors.

Recommendation II.F. *Consumers should have the right to file complaints related to privacy and security of their PHRs and be afforded processes to address their complaints.*

III. Additional Protections for Information in PHRs

Recommendation III.A. *Disclosures of information from PHRs to insurers or employers should require explicit consent immediately prior to disclosure to reduce the risk of unlawful or unfair discrimination.*

NCVHS heard testimony from consumer groups and privacy advocates about the possibility that information may be used to unlawfully or unfairly discriminate against a consumer in such areas as employment or insurance. Because it is difficult to police against discrimination, and because consequences (such as a loss of employment or denial of insurance) can be severe, consumers must give explicit consent to these disclosures at the time they are made, rather than at the time that a consumer signs up for a PHR or when information is transferred into the PHR. This does not apply to uses and disclosures to carry out treatment, payment, or health care operations that are permitted by the HIPAA Privacy Rule.[12]

Recommendation III.B. *Disclosures of a consumer's information for purposes of marketing or in exchange for financial remuneration, directly or indirectly, should require explicit consent immediately prior to disclosure.*

NCVHS heard testimony that consumers are especially concerned about the disclosure of their information for marketing purposes. On the other hand, testimony also indicated that consumers may want to receive information about treatments or other services that are available to them. Accordingly, the disclosure of information for marketing should be prohibited, unless the consumer has given explicit consent to any disclosure for marketing purposes. This recommendation parallels the HIPAA Privacy Rule's requirement for marketing disclosures of protected health information.[13]

[12] 45 C.F.R. § 164.506 (2009).
[13] 45 C.F.R. § 164.508(a)(3)(2009).

Nonetheless, advertising is an important revenue source for some PHR suppliers. Advertising may also convey helpful information to consumers about their conditions or treatments. This principle does not, therefore, require explicit consumer consent at the point advertising occurs on the PHR site. Consumers should, however, be informed at the time they establish a PHR whether advertising will be part of the PHR design, as this may affect their choice to sign up for the PHR in question. Under no circumstances should the PHR design allow consumers to follow an advertising link outside the PHR site in a manner that reveals their identities to advertisers, without explicit warnings and consent at the time the advertising link is followed.

Recommendation III.C. *PHR products should be designed to allow consumers to identify designated categories of sensitive health information. The consumer should then have the ability to control the use and disclosure of the information in these sensitive categories (including in emergency situations).*

NCVHS previously recommended that when information in medical records is transferred for purposes of treatment via the NHIN, individuals should be able to request sequestering of certain defined categories of sensitive health information. In our February 20, 2008, letter to Secretary Leavitt, we said, "[t]he design of the NHIN should permit individuals to sequester specific sections of their health record in one or more predefined categories."[14] Examples of such categories include: domestic violence, genetic information, mental health information, information about reproductive health, and substance abuse. Similar design functionality should also exist in PHRs, but with the ability vested in the consumer to determine whether a health care provider may "break the glass" to access the categories of sensitive information in emergency situations.

IV. Uniform national standards for essential protections for privacy, confidentiality and security in PHRs

Recommendation IV.A. *Consistent with the other recommendations provided herein—and with previous recommendations of NCVHS regarding EHRs—national privacy, confidentiality, and security standards should be established in a manner that supports PHR innovation.*

A primary benefit of PHRs to consumers is the ability to access their health information when they are away from home. Consumers should expect the same level of protections for their information wherever they access it. Presenters at the hearings voiced considerable concern about the difficulties for PHR suppliers who operate in multiple states, when there are differences and inconsistencies in privacy laws among the states.

[14] *See* Letter to Secretary Michael O. Leavitt, "Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment," Recommendation 1a (Feb. 20, 2008).

Although this letter is directed specifically to PHRs, NCVHS also heard considerable concern in testimony about difficulties encountered by providers operating in multiple states when EHRs are subject to differences and inconsistencies in privacy laws among the states. As the NHIN develops, the need for national uniformity is likely to increase. NCVHS has previously recommended that "privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools."[15] Because of the interplay between PHRs and EHRs, NCVHS believes that there should be common national privacy, confidentiality, and security standards for both EHRs and PHRs, and that these standards will facilitate PHR / EHR integration and use.

V. Security Standards

Recommendation V. *Security standards similar to those that are required for information covered by HIPAA should be extended to PHR suppliers.*

Among witnesses that testified before NCVHS, there was strong consensus about the importance of common security protections for all health information repositories. Information security, quality and integrity should be maintained through the use of appropriate administrative, technical, and physical safeguards. All of the witnesses who commented on this topic felt that the HIPAA administrative, technical, and physical safeguards provide a reasonable framework for PHR suppliers to use. This recommendation does not imply that PHR suppliers are covered entities under HIPAA or that they should be treated as such on other matters.

CONCLUSION

PHRs take multiple and changing forms in today's market and contain increasing amounts of sensitive health information about consumers. The development of consistent and effective protections governing PHRs is of great importance. NCVHS will continue to study this area and to make further recommendations about consumer education and information practices as appropriate.

Sincerely,

/s/

Harry L. Reynolds, Jr.
Chairman, National Committee on
Vital and Health Statistics

[15] Letter to Secretary Michael O. Leavitt, "Privacy and confidentiality in the Nationwide Health Information Network," Recommendation 12 (June 22, 2006).