

February 21, 2008

Honorable Michael O. Leavitt
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Individual control of sensitive health information accessible via the
Nationwide Health Information Network for purposes of treatment

Dear Secretary Leavitt:

This letter recommends that you adopt a policy for the Nationwide Health Information Network (NHIN) to allow individuals to have defined control, in a uniform manner, over the disclosure of certain sensitive health information for purposes of treatment. The discussion and recommendations that follow are based on several critical considerations: protecting patients' legitimate concerns about privacy and confidentiality, fostering trust and encouraging participation in the NHIN in order to promote opportunities to improve patient care, and protecting the integrity of the health care system. Disclosures related to quality, billing, research, and other matters have been or will be addressed in other letters from the National Committee on Vital and Health Statistics (NCVHS).

On June 22, 2006, NCVHS sent you a letter report, *Privacy and Confidentiality in the Nationwide Health Information Network*. Among the 26 recommendations were the following:

R-6. HHS should assess the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means. Decisions about whether individuals should have this right should be based on an open, transparent, and public process.

R-7. If individuals are given this right to control access to the specific content of their health records via the NHIN, the right should be limited, such as by being based on the age of the information, the nature of the condition or treatment, or the type of provider.

In an effort to provide you with greater detail regarding these recommendations, NCVHS undertook additional hearings on April 17, 2007. We heard from experts in

obstetrics and gynecology, psychiatry, substance abuse prevention and treatment, emergency medicine, family practice, and internal medicine, as well as from a representative of a regional health information organization (RHIO) and a privacy expert who has studied international approaches to these issues. NCVHS has had extensive deliberations on these matters.

We have concluded that NHIN policies should permit individuals limited control, in a uniform manner, over access to their sensitive health information disclosed via the NHIN. Public dialogue should be undertaken to develop the specifics of these policies, and pilot projects should be initiated to test their implementation. In this letter, we discuss our reasoning in more detail and present our recommendations regarding the following elements of individual control: (1) identification of categories of sensitive health information; (2) optional sequestering of certain categories; (3) notations to health care providers of sequestered health information; (4) implementation of computer-based decision support; and (5) provisions for emergency access to all of an individual's health information.

The Importance of Individual Control

Our goals in developing these recommendations are to improve patient safety and quality of care while developing a network that is practical, affordable, and inclusive, and protects the confidentiality of individual health information.

The development of networks of longitudinal, comprehensive, and interoperable electronic health records (EHRs) presents great opportunities for enhancing coordination of care, avoiding duplication of services, and improving the effectiveness and efficiency of health care. It also makes it possible for all health care providers who may be consulted to have access to an individual's health records from all current and past providers. Consequently, every physician, nurse, dentist, pharmacist, chiropractor, optometrist, physical therapist, and numerous other health care providers and their staffs could have access to the totality of an individual's health records from birth to the most recent encounter at any patient visit. Furthermore, health care providers may obtain patient records without any notice to or permission from the individual, because, under the HIPAA Privacy Rule, disclosures for treatment do not require authorization.

The electronic network model of health information exchange represents a major shift from the decentralized, disconnected, largely paper-based health record system currently in use. There are significant implications for individual privacy and confidentiality due to this shift. Unless specific, privacy-enhancing measures are designed into the networks, individuals could have significantly less privacy than they currently have and that they may reasonably expect would continue with EHR networks. With proper privacy-enhancing measures, however, we believe individual privacy will be reasonably protected across the NHIN.

NCVHS recommends enhancing the privacy protections of individual health information by affording individuals limited control over disclosure of sensitive health information among their health care providers via the NHIN. We believe this approach is compatible with improving the quality of health care, promoting patient trust in the health care system, and safeguarding public health. NCVHS heard testimony from a number of sources indicating the importance of protecting privacy to patient trust in an electronic health care environment. For example, a representative of the substance abuse treatment provider community testified that “the NHIN has the potential to expose sensitive information about an already vulnerable and stigmatized population.” The American College of Obstetrics and Gynecology testified that “the degree to which patients can have control over the information in their records that is accessible by the NHIN is central to the operation and usefulness of the system.”

NCVHS heard testimony that in the U.S. and foreign health care systems where individuals have the right to put restrictions on disclosure of sensitive health information, people rarely elect to do so, but they strongly value having the right and ability to do so. Furthermore, there is a strong public interest in encouraging individuals to seek prompt treatment for sensitive health conditions, such as domestic violence, sexually transmitted diseases, substance abuse, and mental illness. If individuals fear that they have no control over such sensitive health information or that they cannot trust that their sensitive health information will be protected from unwanted disclosure, they might fail to divulge sensitive information relevant to their care, fabricate answers to sensitive questions, or even avoid seeking timely health care altogether, thereby endangering their own health, and possibly the health and safety of others.

Sequestering Information in Sensitive Categories is a Reasonable Solution

NCVHS considered various options and concluded that affording individuals the opportunity to restrict the flow of their personal information by categories is the most promising alternative.

NCVHS recommends permitting an individual to sequester sensitive information based on predefined categories of information as discussed below. Every individual would have the option of designating one or more of the categories for sequestering. If a category is selected, all of the information in that category, as the category is defined, would be sequestered. The individual would not have the option of selecting only specific items within that category to sequester (an approach discussed below that we rejected). If a category is so designated, then health care providers accessing the individual’s EHR via the NHIN would not see any information in the selected categories. The individual would have the further option of providing consent to a health care provider to access the sequestered information. There are numerous technical solutions possible for how to provide this additional consent, and the optimal one should be determined as a design matter.

The approach of separating certain categories of sensitive health information is consistent with and already required by federal law regarding the confidentiality of alcohol and drug abuse treatment records. HHS regulations, 42 CFR Part 2, provide that a program receiving federal financial assistance generally may not use or disclose any information about an individual who has applied for or been given diagnosis or treatment for alcohol or drug abuse without the individual's express consent, with limited exceptions. Other federal and state laws and regulations also restrict disclosure of HIV test results, genetic test results, and other information. At our hearing on April 17, 2007, an expert on health information privacy testified that approaches to sequester sensitive health information are being developed in Canada, England, and the Netherlands. Some international standard setting organizations and experts in the public and private sectors are also considering this approach.

NCVHS recognizes that individuals differ in their opinions about what categories of health information should be considered sensitive. We also recognize that designating particular categories, and, even more critically, defining what information is included in each category, will be a complex and difficult undertaking. There are many considerations to accommodate the array of opinions and values as to what constitutes sensitive information, and these may vary depending on an individual's diagnoses, age, socio-economic position, cultural upbringing, religious beliefs, or other personal circumstances. Nevertheless, NCVHS believes that it is important to designate categories of sensitive health information with precise definitions. It is also important to address the policy and technical issues involved in changes to designations over time.

Having uniform definitions of sensitive health information across the NHIN will be critical to establishing a solution that works well in a society where people travel frequently and receive care from multiple health care providers. Careful consideration should be given to which categories are selected and the granularity with which patients can choose to designate information to sequester. Too many categories, or definitions which are too broad, might inadvertently cause patients to exclude critical information necessary for treatment. Providers could end up requesting access to the sequestered information during each visit, thereby reducing efficiency and undermining the purpose of the privacy protections. Too few categories, or categories that are defined too narrowly might cause sensitive information to be made available to all health care providers, possibly causing patients to avoid seeking treatment out of fear that this sensitive information would not be adequately protected.

We have listed below some categories of health information that are commonly considered to contain sensitive information. Federal and state laws and regulations already require separation of some of these categories of health information from other health information, so there is considerable experience with at least some types of sensitive information. However, NCVHS recognizes that selecting a list of categories and defining such categories will need considerable attention. The process of developing such a list must be open and transparent and give due consideration to existing state and federal laws, as well as professional and accreditation standards. NCVHS believes that a public process for addressing these issues is essential.

Example Categories

Genetic information — This category might include such information as genetic test results, genetic counseling reports, diagnoses of specifically designated genetic disorders, and interventions to deal with those genetic disorders.

Mental health information — This category might include information about signs, symptoms, and diagnoses of mental health illness, or therapies.

Reproductive health — This category might include information about reproductive history, sexual behavior, sexually transmitted diseases (including HIV), fertility, and pregnancies.

Domestic violence — This category might include information about a history or current record of child abuse, partner abuse, or elder abuse, including location information for patients who are victims of domestic violence.

Substance abuse — This category might include information about a history or current record of alcoholism, abuse of licit or illicit drugs, treatment for such a condition, or any information that might identify an individual as a substance abuser.

Through testimony and Committee discussion, legitimate concerns were raised about how sequestering categories of health information would affect medical malpractice liability. Liability could potentially be affected in at least three ways. The sequestration of critical information might cause providers to give less than optimal advice or treatment because critical information is not considered. On the other hand, without sequestration or other limits on the scope of health records, the potential for liability could increase because a provider might be held responsible to know and take into account every detail of a patient's health history available via the NHIN. Finally, liability may also be implicated as a result of violations of confidentiality due to imperfect sequestration of data by a provider or the provider's system. The implications for liability deserve additional consideration.

Notations of missing data for Health Care Providers

When patients are provided an opportunity to choose categories of information for sequestration, NCVHS believes that it is important that a notation is made to the provider that some information in the record is not being made available at the request of the patient. We understand that it is possible that a notation in the record might reveal more information than would be available under current practice. For example, the HHS regulations regarding substance abuse treatment do not give a provider information about the sequestration of a record of substance abuse treatment. In the fragmented health records system we have today, moreover, patients can withhold information from their providers and be reasonably confident that the information will not be disclosed.

Nevertheless, NCVHS concluded that, where permitted by law or regulation, health care providers should be notified when information is being sequestered in order to increase providers' trust in the contents of the record. If a provider knew that patients could sequester information but they would not be notified, providers could never really trust that their records were accurate and complete, and would be hesitant to treat patients based on those records. The inclusion of some notation that information is missing alerts a provider that caution and special care are appropriate. Furthermore, a significant advantage of the notation is that it provides an opportunity for providers to discuss with their patients concerns about the sequestration of information and the resulting impact on their health care.

There are at least two approaches to how the notation should be accomplished. One solution would be to give a general notice that information has been sequestered without any indication of what categories were designated by the patient. This approach potentially increases privacy for the patient because the nature of a category, such as mental health information, might, by itself, reveal the sequestered information. For routine care, a care provider might not need to see the sequestered information and most of the time it would remain hidden. A disadvantage of this approach is that it may require health care providers to question patients about every category routinely in an attempt to determine whether any relevant information is missing, increasing the burden on providers and ultimately resulting in a system less protective of privacy and less efficient.

Another approach is that the sequestered category should be noted, permitting the provider to make a more informed judgment as to whether the category is likely to be relevant to the current encounter, and only to ask the patient when it seems appropriate. This approach has the potential to be more efficient, and, since most of the time sequestered information would remain hidden, it could adequately protect the patient's privacy. A disadvantage of this approach is that some categories, by themselves, reveal sequestered information, such as that a patient has a mental health or substance abuse record, and designations of specific categories of sequestered information would not be adequately protective of patient privacy.

NCVHS acknowledges that it does not yet know exactly how such a notation process would work. The success of the process will likely depend on the enumerated categories, the breadth of their definitions, and the frequency with which patients sequester information. These are the types of issues that should be explored in future hearings and investigated through pilot projects and research.

Emergency access

In an emergency where a patient is unable to give or refuse consent to access sequestered health information, such as when an unconscious patient is treated in an emergency department, it may be essential to have the individual's complete health information. NCVHS believes that all health information should be available on an

emergency basis through an electronic “break the glass” feature to permit access to the patient’s complete health information, including sequestered information.

If this feature is used, an audit trail should record the specifics of the incident, and it should automatically trigger a review by health privacy officials at the health care facility. The patient or the patient’s representative also should be notified as soon as possible that the “break the glass” feature was used. NCVHS believes that an emergency access provision is consistent with the concept of implied consent to treat in emergencies and that it promotes the strong societal interests in providing essential treatment.

Re-sequestration of Sensitive Information

Once sequestered information has been accessed (either pursuant to a patient’s authorization or based on emergency access), the treatment of the information as sensitive should be continued in future exchanges of records across the NHIN unless otherwise consented to by the patient.

Should a provider access information that had been sequestered by the patient, the provider should be required, after the encounter, to ensure that the categories of information identified by the patient for sequestration continue to be sequestered when the patient’s record is shared via the NHIN. Again, it is important to address the policy and technical issues involved in implementing these provisions.

Recommendations Regarding Sequestration

The first recommendation has several parts all of which must be taken together in order to meet the principles of quality, safety, and protection of confidential health information.

Recommendation 1a. The design of the NHIN should permit individuals to sequester specific sections of their health record in one or more predefined categories. The list of potentially sensitive categories and their contents should be defined in national basis so that it is uniform across the NHIN.

Recommendation 1b. HHS should initiate an open, transparent, and public process to identify the possible categories of sensitive information for sequestration by individuals and to define with specificity the criteria for inclusion and exclusion within each category. The process should take into account both patient concerns about privacy and the concerns of health care providers about quality of care.

Recommendation 1c. When a health care provider accesses health information with one or more categories sequestered, a notation should indicate that sensitive health information has been sequestered at the direction of the patient. The specificity of the notation will need to be determined.

Recommendation 1d. The design of the NHIN should permit individuals to authorize selected health care providers to access sequestered health information.

Recommendation 1e. EHRs transmitted via the NHIN should contain a “break the glass” feature enabling health care providers to access an individual’s complete health information, including sequestered information, in the event of a medical emergency.

Recommendation 1f. If a health care provider obtains emergency access to sequestered information, a description of the circumstances surrounding access should be part of the audit trail, and the health care entity’s designated privacy official should be notified automatically.

Recommendation 1g. If a health care provider obtains emergency access to sequestered health information, the patient or the patient’s representative should be notified promptly.

Recommendation 1h – If a health care provider obtains access to sequestered health information, the provider is responsible for taking whatever action is required to continue to protect the stated privacy preferences of the patient.

NCVHS would be pleased to work with the Department to hold hearings and provide a public process for addressing these issues.

Other Options We Considered

NCVHS considered various options for limiting disclosure of sensitive health information, but, for the reasons described below, none of the others was considered as promising as restriction by categories.

No sharing restrictions. One possibility would be for a Health Information Exchange (HIE) not to restrict the disclosure of information, including sensitive health information, available over the network except where legally required. NCVHS heard testimony from one longstanding RHIO that took this approach. Its rationale was that segregating sensitive information would be administratively difficult in light of the

RHIO's capabilities. While recognizing this as a locally successful approach, NCVHS recommends that on a national basis it is necessary to explore methods to increase patients' control when their information is shared via the NHIN.

Restriction by type of provider. NCVHS next considered whether health information should be classified as sensitive based on the type of provider or setting for care. Although this approach appears relatively simple to implement, it affords insufficient protection to sensitive health information, which is often commingled with primary care records whether in a primary care or specialty practice. For instance, much sensitive health information (e.g., mental health information) is maintained by physicians in general practice, but would not fall into a category afforded special protections. In addition, some specialty practitioners, such as gynecologists, also provide primary care; thus, exclusion of their records would reduce the availability of much non-sensitive health information.

Restriction by age of information. NCVHS discussed the possibility that information could be available only if it were fairly recent, with data after a certain time period not automatically included in the initial view of the patient's record. Most clinical decisions are made based on the most recent information available about the patient, such as recent diagnoses, procedures, and current medications, and much information older than, for example, 10 years is not critical. In this model, all recent information would be presumptively available to any treating provider, but information older than a set period of time would be available only via some further consent mechanism. Although some of the presumptively available fields might include information deemed sensitive, such as medications used in psychiatric treatment, much out-of-date and irrelevant data would be kept private. We rejected this as the sole manner in which to protect information because (1) it is not sufficiently protective of certain sensitive information; (2) a standard length of time by which to measure the age of data would have to vary with the age of the individual; (3) for individuals with chronic conditions, the long-term history of an illness may be important; and (4) certain diagnoses and treatments retain clinical significance despite the passage of time.

Item-by-item restrictions. Another possibility would be to permit individuals to include or exclude any specific item of their health information when a record is transferred to a health care provider. Although this approach would increase patient control, it would be difficult to determine what limitations, if any, to apply, and it would undermine the confidence of health care providers in the integrity and utility of health information. We also believe that the privacy protection intended by such granular control by individuals can be achieved through sequestering by category.

Restricting everything but predetermined fields. NCVHS also considered the feasibility and desirability of developing a master clinical summary for all patients that would be the starting point for providers to build their own record. With this model, a set group of data fields (e.g., name, birth date, recent diagnoses, recent procedures, current medications, allergies, immunizations) would be presumptively available to any treating provider. Other information would be available only via some further consent

mechanism. Although some of the presumptively available fields might include information deemed sensitive, such as medications used in psychiatric treatment, most health information would be kept private. NCVHS recognized this approach as practical, but rejected it because it would require substantial supplementation by each health care provider who renders ongoing, non-emergency care, and thus would be inadequate for many health care settings. It also may not protect privacy adequately because it presumptively discloses certain sensitive health information.

Clinical Decision Support

Clinical decision support (CDS) is an important element of EHR systems and HIEs. The relationship between CDS and sequestration of sensitive health information has not yet been explored to any significant degree. For example, it is not clear what the potential risks and benefits would be if CDS were to search categories of sequestered information (e.g., for possible drug interactions) when the sequestered information is not available to the clinician.

Recommendation 2. HHS should monitor developments in the relationship between clinical decision support and sequestered health information and determine if or when pilot projects, trial implementations, or other research measures are warranted.

Research, Development, and Implementation

NCVHS recognizes that the technologies and human factors needed to implement the recommendations in this letter are not necessarily readily available for the EHR systems, HIEs, and other components of the emerging NHIN. We understand that much work will be needed to select the categories of sensitive health information and to develop definitions and inclusion and exclusion criteria for the various categories of sensitive health information. Furthermore, a process needs to be established for ongoing research, development, implementation, evaluation, and refinement of methods for sequestering categories of sensitive health information. We realize that it will never be possible to have a system that perfectly sequesters only an individual's sensitive health information. Nevertheless, we strongly believe that the principles presented in this letter are conceptually sound, substantially achievable over time, and form a reasonable option to simultaneously protect privacy and confidentiality, enable optimum health care, and encourage patients not to avoid care simply to protect information they consider sensitive.

NCVHS also recognizes that the sequestration of sensitive health information by category in EHRs represents a new model of clinical care. Various health care providers might be understandably concerned about the implications of an incomplete record for the quality of patient care and this concern must be addressed as well. More than technological solutions will be needed to make this new arrangement successful. It will

require substantial public and professional education as well as policies and procedures that consider the medical, social, psychological, cultural, and personal factors in patient care.

Recommendation 3. HHS should support research, development, and pilot testing of technologies and tools for sequestering designated categories of sensitive health information transmitted via the NHIN.

Recommendation 4. HHS should support research, development, and pilot testing of public and professional education programs needed to implement the sequestration of sensitive health information.

Recommendation 5. HHS should support the ongoing study of the consequences of sequestration of sensitive health information, including potential liability issues and the human factors necessary for successful implementation.

Individual control of sensitive health information is one of the most important privacy issues to be resolved in developing and implementing the NHIN. The recommendations in this letter calling for additional public input, a deliberative process in policymaking, and pilot projects reflect our judgment that these issues are complicated, contentious, and crucial. National policies on individual control of sensitive health information accessible via the NHIN for purposes of treatment must be developed in a way that both enhances health care and protects privacy. These policies also need to be developed before the local and regional components of the NHIN finalize the designs of their systems and business models. Accordingly, NCVHS respectfully urges HHS to begin addressing these issues expeditiously. The process remains ongoing and NCVHS would be pleased to continue its active involvement.

Sincerely,

Simon P. Cohn, M.D., M.P.H.
Chair, National Committee on
Vital and Health Statistics