NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Privacy Report

Recommendations on Privacy and Confidentiality, 2006—2008

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Recommendations on Privacy and Confidentiality, 2006—2008

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Hyattsville, Maryland
May 2009

Contents

Introduction

The National Committee on Vital and Health Statistics (NCVHS) has advised the Secretary of the U.S. Department of Health and Human Services (HHS) on health information matters for nearly 60 years. The NCVHS Subcommittee on Privacy and Confidentiality was formed in 1996 as the result of the enactment of the Health Insurance Portability and Accountability Act (HIPAA).[1]

Initially, the Privacy and Confidentiality Subcommittee focused its efforts on providing advice regarding the development, enforcement, assessment, and modification of the HIPAA Privacy Rule and it will continue this role, as mandated by law.

Since 2005, however, it has turned much of its attention to the privacy and confidentiality considerations associated with the development and operation of a Nationwide Health Information Network (NHIN). This new focus was created in part in response to a request from the National Coordinator for Health Information Technology.

NCVHS believes that the public has much to gain from interoperable healthcare systems, as long as appropriate privacy protections are provided. NCVHS also believes that support depends on public confidence and trust that personal health information will be protected from misuse and inappropriate disclosure. Because the HIPAA Privacy Rule predates substantive discussion regarding the establishment of the NHIN, many entities now involved in collecting, storing, and exchanging personal health information are not covered by the Privacy Rule.

The Committee's extensive study of these issues in recent years has led to three letter-reports to the Secretary of Health and Human Services proposing ways to enhance public trust in, and public benefit from, the electronic exchange of personal health information. Taken together, these NCVHS letter-reports advance a broad set of consistent privacy principles that the Committee believes should be built into the NHIN as it is developed, as well as into future federal health information privacy laws. The letter-reports are:

- Privacy and Confidentiality in the Nationwide Health Information Network (June 2006)
- Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices (June 2007)
- Individual Control of Sensitive Health Information Accessible via the Nationwide Health Information Network for Purposes of Treatment (February 2008)

This monograph was created to make the National Committee's recommendations on privacy, confidentiality, and the NHIN available in a convenient format for all who have an interest in understanding the considerations related to the privacy and confidentiality of personal health information within the NHIN. The Committee continues to be actively involved in studying privacy issues, and will generate additional letters, reports, and recommendations as needed in the future.

[1]The Subcommittee's name was changed to the Subcommittee on Privacy and Security in May 2008.

June 2006: A Broad Review of Privacy, Confidentiality, and the Nationwide Health Information Network

The first National Committee on Vital and Health Statistics (NCVHS) letter-report covered a wide range of topics that are central to safeguarding personal health information in the Nationwide Health Information Network (NHIN). The Subcommittee on Privacy and Confidentiality developed its analysis and recommendations through an 18-month process of learning and deliberation that included three hearings in various locations across the United States, conference calls, public meetings, and thorough discussions with the full National Committee.

The letter-report addressed the following topics:

- The role of individuals in making decisions about the use of their personal health information;
- Policies for controlling disclosures across the NHIN;
- Regulatory issues such as jurisdiction and enforcement;
- Use of information by nonhealth care entities; and
- Establishing and maintaining the public trust necessary to ensure the success of the NHIN.

The letter-report called attention to concerns about electronic health records (EHRs) and the NHIN that make it essential that HHS and other public and private entities begin "immediate, substantial, and sustained efforts to establish and maintain public trust in the NHIN." It conveyed 26 recommendations in 10 areas: flexibility vs. uniformity; participation; individual control; disclosure; jurisdiction, scope, and relationships with other laws; procedures; enforcement; uses by third parties; relationship to the HIPAA Privacy Rule; and establishing and maintaining public trust.

I. Privacy and Confidentiality in the Nationwide Health Information Network

June 22, 2006

The Nationwide Health Information Network (NHIN), on which the U.S. Department of Health and Human Services (HHS) is taking the lead, has the potential to enhance health care quality, increase efficiency, and promote public health. The NHIN also creates new challenges to and opportunities for safeguarding health privacy and confidentiality.

The National Committee on Vital and Health Statistics (NCVHS) has carefully considered the implications of the NHIN for health privacy and confidentiality. This report is based on a series of five hearings in 2005 held by the NCVHS Subcommittee on Privacy and Confidentiality. Three hearings were held in Washington, and one each in Chicago and San Francisco. Each hearing focused on different individuals and groups concerned about health information privacy and confidentiality, including hospitals, providers, payers, medical informatics experts, ethicists, integrated health systems, Regional Health Information Organizations (RHIOs), and consumer and patient advocacy groups. We also heard testimony from representatives of nationwide health networks in Australia, Canada, and Denmark. The Subcommittee then held a series of meetings open to the public and telephone conference calls to discuss its findings and prepare a report for the Committee to submit to HHS.

This report contains the following seven sections: (A) Definitions; (B) The Importance of Privacy and Confidentiality; (C) The Role of Individuals; (D) Controlled Disclosure of Personal Health Information; (E) Regulatory Issues; (F) Secondary Uses of Personal Health Information; and (G) Establishing and Maintaining Public Trust.

A. Definitions

One issue that often clouds discussions regarding privacy is the difficulty of differentiating among "privacy," "confidentiality," and "security." These terms are often used interchangeably and imprecisely. In this report, we have adopted definitions from the recent Institute of Medicine publication, "Disposition of the Air Force Health Study" (2006):

- Health information *privacy* is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.
- *Confidentiality*, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.
- *Security* is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

Although a discussion of the appropriate security controls for the NHIN is beyond the scope of this report, security must be addressed for the NHIN to be successful. The security of electronic health records (EHRs) and the NHIN may be addressed in a future report of NCVHS.

We use the term "personal health information" rather than "protected health information" because the latter is a term of art in the Privacy Rule promulgated under the Health Insurance Portability and Accountability Act (HIPAA), and we want to use a term not constrained by HIPAA coverage. The report also uses the term "individual" rather than "patient" in many places because not all health care providers (e.g., pharmacists) have a "provider-patient" relationship with the individuals they serve.

B. The Importance of Privacy and Confidentiality

Informational privacy is a core value of American society. Public opinion surveys consistently confirm the value of privacy to the public. Many individuals believe that there are certain matters that they do not want to share widely, or at all, even with friends, family members, or their physicians. Similarly, many people are quite concerned about the potential ramifications if employers, insurers, and other third parties have access to their personal information, including personal health information.

Privacy and confidentiality are neither new concepts, nor absolutes. Since the time of Hippocrates, physicians have pledged to maintain the secrecy of information they learn about their patients, disclosing information only with the authorization of the patient or when necessary to protect an overriding public interest, such as public health. Comparable provisions are now contained in the codes of ethics of virtually all health professionals.

As a practical matter, it is often essential for individuals to disclose sensitive, even potentially embarrassing, information to a health care provider to obtain appropriate care. Trust in professional ethics and established health privacy and confidentiality rules encourages individuals to share information they would not want publicly known. In addition, limits on disclosure are designed to protect individuals from tangible and intangible harms due to widespread availability of personal health information. Individual trust in the privacy and confidentiality of their personal health information also promotes public health, because individuals with potentially contagious or communicable diseases are not inhibited from seeking treatment.

One of the major weaknesses of the current system of largely paper-based health records is its incomplete and fragmented nature. Ironically, this fragmentation has the unintended consequence of preventing disclosure of personal health information. Precisely because comprehensive health information is difficult to access, compile, use, and disclose, some health information privacy and confidentiality may be achieved by default. Nevertheless, individuals pay dearly for this indirect protection in terms of unavailability of vital information in emergencies, difficulty in maintaining continuity of care, adverse health outcomes due to prescribing and other errors, waste of health care resources, and inability to compile aggregate data on health measures and outcomes. Thus, there are ample ethical, policy, and economic reasons

for a shift to EHRs and an interoperable network of EHRs, so long as there are reasonable privacy and confidentiality measures.

People differ widely in their views regarding privacy and confidentiality, and individual opinions may be influenced by the individual's health condition as well as cultural, religious, or other beliefs, traditions, or practices. By providing individuals with reasonable choices concerning the uses and disclosures of their personal health information, the health care system and society demonstrate respect for persons. Furthermore, limiting excessive and unnecessary disclosure of personal health information helps to prevent health-based discrimination.

In an age in which electronic transactions are increasingly common and security lapses are widely reported, public support for the NHIN depends on public confidence and trust that personal health information is protected. Any system of personal health information collection, storage, retrieval, use, and dissemination requires the utmost trust of the public. The health care industry must commit to incorporating privacy and confidentiality protections so that they permeate the entire health records system.

NCVHS recognizes the difficulty in balancing the interests of privacy and confidentiality against the health care, economic, and societal benefits of the NHIN. Nevertheless, individual and societal interests are not necessarily inconsistent. There is a strong societal interest in privacy and confidentiality to promote the full candor on the part of the individual needed for quality health care. At the same time, individuals have a strong interest in giving health professionals the ability to access their personal health information to treat health conditions and to safely and efficiently operate the health care system. Both the society as a whole and each individual have an interest in improvements in public health, research, and other uses of personal health information.

Throughout our hearings and in drafting this report and recommendations, it became clear to the members of NCVHS that devising and establishing a NHIN involves difficult tradeoffs. As the availability of personal health information increases with new applications of technology, the utility of information increases, but so does the risk to privacy and confidentiality.

C. The Role of Individuals

The most difficult and contentious privacy and confidentiality issues are those surrounding whether and how individuals should have (1) choice over participation in the NHIN and (2) ability to control access to the contents of their health records accessible over the NHIN.[2] Addressing these difficult issues is further complicated because the specific structure of the NHIN has yet to be determined. For example, will the NHIN include storage of data, provide only the transport mechanism for moving data from place to place, or merely allow remote access to view data over a network? Without knowing the technical architecture or organizational plan of the NHIN, it is difficult to know what it means for an individual's records to be "accessible through" or "a part of" the NHIN.

[2] See the Committee's February 2008 letter and recommendations on individual control, page 25.

Flexibility or uniformity?

Deciding on the appropriate level of individual control over personal health information accessible via the NHIN involves balancing important interests, such as the desire of some individuals to be able to control their personal health information and the need to document accurately medical history and treatment; the desire for a system that is flexible and the need to avoid a system that is too complicated; the desire to increase individual choice, and the desire to reduce complexity and the costs imposed on providers, payers, and other stakeholders.

Satisfying the desire of those who wish to promote individual choice and individual control suggests an NHIN with great flexibility. However, since there is a direct relationship between flexibility and complexity, too many choices could create a health information system that is overly complex; unwieldy to navigate; and needlessly expensive to design, implement, or operate. Too much flexibility might also result in individuals inadvertently withholding information necessary for appropriate treatment. Incomplete personal health information could jeopardize the improvement in individual and population health outcomes that provide a major justification for establishing the NHIN.

On the other hand, in an environment that lacks the flexibility to accommodate a variety of individual choices, privacy and confidentiality protections would be ineffectual. In such an environment, the public may be reluctant to support the establishment of the NHIN. Furthermore, individuals concerned about a lack of privacy and confidentiality might not disclose all relevant information to their health care providers, and some individuals might forego health care altogether.

An initial issue is whether individuals should have the right to continue having their personal health information maintained only on paper records. NCVHS heard testimony on the issue from several witnesses. We conclude that although individuals should have reasonable control over the collection, use, and disclosure of their personal health information, the method by which their personal health information is stored by their health care providers should be left to the health care providers. Increasingly, records are being maintained in electronic form, and inevitably, that practice will continue and expand.

Recommendation on flexibility or uniformity:

I-1. *The method by which personal health information is stored by health care providers should be left to the health care providers.*

Mandatory or voluntary participation?

The next issue to consider is whether participation in the NHIN should be mandatory. NCVHS believes that individuals should have a choice about whether to participate in the NHIN. Although we recognize that a system of mandatory participation would be easier, less costly, and more comprehensive, the Committee believes that these expected benefits do not justify the burden on individual privacy and confidentiality. In addition to the likely loss of political support if participation were mandatory, a loss of public health benefits is possible should individuals forego medical care because of privacy concerns. Accordingly, health care providers should not be able to condition treatment on individuals agreeing to have their health records accessible via the NHIN.

There are two basic approaches for giving individuals the choice of whether to have their personal health records accessible via the NHIN: opt-out and opt-in. Under the opt-out approach, an individual's personal health information is presumed to be available to authorized persons via the NHIN, but any individual may elect not to participate. The advantages of this approach are that it may be easier, less costly, and result in greater participation in the NHIN. The other approach, opt-in, requires that health care providers obtain the explicit permission of individuals before allowing their information to be available via the NHIN. Without this permission, an individual's personal health information would not be accessible via the NHIN. The opt-in approach increases individual autonomy, but is more administratively burdensome and may result in fewer individuals participating in the NHIN. While NCVHS supports the principle of choice, we were unable to agree whether to endorse an approach as to how individuals should exercise this choice.

Under either approach, however, understandable and culturally sensitive information and education are needed to ensure that individuals realize the implications of electing or declining to participate. An individual's decision about participating in the NHIN should be the knowing exercise of an important right and not just another paper to sign to obtain health care.

Recommendations on mandatory or voluntary participation:

I-2. *Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN.*

I-3. *Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN.*

I-4. *HHS should monitor the development of opt-in or opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social, and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate.*

I-5. *HHS should require that individuals be provided with understandable and culturally sensitive information and education to ensure that they realize the implications of their decisions as to whether to participate in the NHIN.*

The nature of individual control

Once an individual elects to make his or her information accessible via the NHIN, the next question is whether the individual should have the right to control access to specific portions of his or her record disclosed via the NHIN and, if so, the specifics of that right. NCVHS grappled with the question of whether the same rules regarding individuals' rights to control access to their health records accessible via the NHIN should also apply to the source of those health records originating with the health care provider. Although in the following text we describe the arguments that NCVHS heard on this matter during our hearings, NCVHS does not take a position on this issue. Nevertheless, we believe that this issue might become increasingly important.

Proponents of the view that individuals should not be permitted to control the contents of their health records raise three main arguments. First, they assert that such a policy is essential to maintain the integrity of the contents of the individual's health record. Current standard health information practices, some state laws, and widely adopted health professional standards require that any changes to the contents of a health record must be made through an amendment process and not by removing or deleting any information in the original record. Second, giving individuals the right to limit access to certain portions of their health record may interfere with the ability of their providers to make appropriately informed decisions. The concern is that individuals may not have the knowledge to discern what information in their health record can be blocked from access without affecting important decisions regarding their care. Third, NCVHS heard testimony from some health care providers

who were concerned about possible malpractice liability stemming from errors in health care caused by accessing incomplete or filtered personal health information via the NHIN.

On the other hand, there are three main arguments in favor of granting individuals broader rights to control disclosure of their health records via the NHIN. First, proponents of this view assert that many health records contain sensitive, old information that is not relevant to a current clinical decision. Today, this information is often not available to all health care providers because of the fragmented nature of the health records system. However, under a functioning NHIN, sensitive, potentially embarrassing information would remain accessible indefinitely, possibly leading to stigma, humiliation, or even discrimination. This argument holds that a new health records system should not afford less protection for privacy and confidentiality than is presently afforded indirectly by the current, fragmented, largely paper-based system.

In line with the tradition of a patient's right to control what treatments to accept or refuse, advocates of this position believe that individuals should have the right to withhold information, even if it may result in bad outcomes. Second, individuals with sensitive medical conditions, such as substance abuse, mental illness, and sexually transmitted diseases, may be reluctant to seek treatment if they cannot be assured of controlling access to their personal health information. Thus, the argument is that individuals might forego treatment, thereby endangering their own or even the public's health. Third, NCVHS heard testimony that so long as health care providers have ready access to a standard set of essential information, such as current diagnoses, medications, allergies, and immunizations, emergency care can be rendered adequately and additional personal health information or permission to access additional personal health information can be obtained from the individual.

The degree of individual control

If individuals are given the right to control access to the contents of their health records, the next question is what degree of control should they have? Should they have the right to prevent access to any element in the record or only some elements? On the one hand, giving individuals unlimited control is one way to empower them. On the other hand, if individuals had unfettered control, health care providers would likely place less confidence in the accuracy and completeness of the records. A foreseeable result might be that instead of reducing duplication of effort, the new health record system could require every provider to obtain a new history and new individual information. Furthermore, most individuals would lack the expertise to determine which parts of their health record were relevant to current clinical decisions and would risk inadvertently excluding information to the detriment of their own health. For these reasons, if individuals are given the right to control access to their records, the right should be limited.

Methods of individual control

There are various ways in which individuals' rights to control access to their health records could be limited. For example, they could be based on the age of the personal health information (e.g., access could be denied only to records over 10 years old), they could be based on the nature of the condition or treatment (e.g., substance abuse, mental illness, reproductive health), and they could be limited by provider type or provider name. In developing a strategy for deciding to what type of information individuals should be permitted to limit access, it is important to consult with health care providers and patient advocates, including those representing culturally diverse populations.

Possible ways of affording individuals the right to control access to certain aspects of their health records include the following three proposals, none of which are necessarily endorsed by NCVHS: (1) the entire records of a particular provider (e.g., psychiatrist) or a class of providers could be kept outside of the NHIN; (2) some parts of a health record could be blocked from access; or (3) some elements of a health record could be deleted altogether from the EHR. Blocking means that the information would still exist, but it will not be seen by health care providers looking at the record unless a provision for overriding blocked information (e.g., in emergencies) or granting certain providers access rights (e.g., allowing only mental health providers to see mental health information) is built into the system. Clinical decision support, however, might be programmed to advise health care providers that, for example, the individual had a prior adverse reaction to a certain class of drugs. Blocked information also could be made available for statistical analyses, data aggregation, quality assurance, and other purposes in deidentified form. If a blocking approach were to be pursued, additional feasibility analyses would be necessary. Deletion carries with it the problems outlined in III C.

NCVHS heard testimony from experts about the Australian, British, Canadian, and Danish health systems that grant individuals the right to block access to certain information. The Deputy Manager of the Danish Centre for Health Telematics testified that in Denmark, this right was rarely exercised, but individuals highly valued having this right. He further testified that he was not aware of any complaints by physicians about this arrangement. However, cultural, social, legal, or scalability differences may make the Danish experience inapposite.

Recommendations on individual control:

I-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.

I-7. If individuals are given the 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.

D. Controlled Disclosure of Personal Health Information

Modern health care is often provided in large institutions with hundreds of employees in dozens of job categories. Not all of the individuals who need access to personal health information need the same level or kind of information. For example, dieticians and health claims processors do not need access to complete health records whereas treating physicians generally do. Protecting the confidentiality of personal health information in such settings requires institutions to establish different access rules depending on employees' responsibilities and their need to know the information to carry out their role. The HIPAA Privacy Rule includes a provision requiring that only the "minimum necessary" protected health information be included for disclosures other than for treatment, to the subject individual, pursuant to that individual's authorization, or where required by law. This minimum necessary standard encompasses role-based access. The principle of "role based access criteria" and the related concept of data classification have already been successfully embodied in the EHR architectures of several large health care organizations and health care systems. We support this principle and believe that it should be a standard for EHRs. We also believe that role based access criteria should be applied to the use and sharing of personal in the NHIN.

Another principle of controlled access applies to the non-medical uses of personal health information. Each year, as a condition of applying for employment, insurance, loans, and other programs, millions of individuals are compelled to sign authorizations permitting employers, insurers, banks, and others to access their personal health information for non-medical purposes. These authorizations are nominally voluntary; individuals are not required to sign them, but if they do not, they will not be considered for the particular job, insurance policy, loan, or benefit. In addition, for most of these authorizations, no limits are placed on the scope of the information disclosed or the duration of the authorization. For example, after a conditional offer of employment, the Americans with Disabilities Act does not prohibit employers from requiring that individuals sign an authorization to release all of their health records, regardless of whether the information disclosed has any relevance to the position for which the individual is under consideration.

An EHR system creates greater risks to confidentiality because the comprehensive disclosures might include much more information than is necessary to the particular decision at hand. At the same time, conversion to EHRs creates an unprecedented opportunity to protect confidentiality. At present, it may not be practicable to search a paper record system to disclose only a certain category of personal. Thus, personal disclosed through compelled authorizations today is routinely overbroad, even where a narrower request is made. Conversion from paper records to EHRs could greatly enhance the confidentiality of personal health information and resolve the problem of excessive disclosures pursuant to authorizations. *Contextual access criteria* could be developed and integrated into the architecture of EHRs and the NHIN to permit disclosure of only the information needed by the user. For example, applying such technology, employers would only get information relevant to a particular job classification, and life insurers would only get information relevant to mortality risk. As a result, only

personal relevant to its intended use would be disclosed pursuant to an authorization.

Developing the methodologies for these proposals will be complex and must involve collaboration by various stakeholders. The failure to incorporate contextual access criteria into the design of the NHIN, however, would have significant negative consequences, because this failure would impede the ability to limit unnecessary disclosures of irrelevant, sensitive personal to third parties. Despite our certainty that contextual access criteria are essential to protecting confidentiality in the NHIN, the NCHVS has been unable to identify any public or private research or pilot projects to develop this technology.

Recommendations on disclosure:

I-8. Role-based access should be employed as a means to limit the personal health information accessible via the NHIN and its components.

I-9. HHS should investigate the feasibility of applying contextual access criteria to EHRs and the NHIN, enabling personal information disclosed beyond the health care setting on the basis of an authorization to be limited to the information reasonably necessary to achieve the purpose of the disclosure.

I-10. HHS should support research and technology to develop contextual access criteria appropriate for application to EHRs and inclusion in the architecture of the NHIN.

I-11. HHS should convene or support efforts to convene a diversity of interested parties to design, define, and develop role-based access criteria and contextual access criteria appropriate for application to EHRs and the NHIN.

E. Regulatory Issues

The NHIN will require a series of regulatory measures to implement privacy and confidentiality protections. These measures fall into the categories of jurisdiction and relationship with other laws, procedures, and enforcement.

Jurisdiction, scope, and relationship with other laws

Several witnesses testified about the confusion, difficulty, and expense of complying with the HIPAA Privacy Rule along with numerous health privacy laws enacted by the states. Conflicts among the various sources of health privacy regulation would likely be even more pronounced with the NHIN. For example, what law would apply to an individual's health records created in states A and B, stored by or accessed through a RHIO in state C, disclosed to an entity in state D for use in state E? A single national standard would facilitate compliance, but the price of uniformity would be a loss in flexibility and the ability of the states to implement policies that reflect local conditions and values. NCVHS is aware that HHS has awarded a contract to the National Governors Association to study the variety of state laws regarding personal health information, and we look forward to the results of that effort. In the meantime, HHS should explore ways to preserve some degree of state variation without losing technical interoperability and essential protections for privacy and confidentiality.

Some of the privacy and confidentiality measures discussed in this report may be inconsistent with certain provisions of the HIPAA Privacy Rule. For example, under the Privacy Rule, individuals have a right to request amendments to their health records, but covered entities may refuse the request. In this report, we note that one option is to give individuals a right to exclude or block information contained in their EHR from being accessed via the NHIN. Adoption of this approach would require amendment of the Privacy Rule. In addition, the rules governing the NHIN need to be harmonized with other relevant federal regulations, including those applicable to substance abuse treatment records.

The purpose of the administrative simplification title of HIPAA was to regulate the process of submitting health care claims. Thus, the HIPAA Privacy Rule was designed to apply only to the covered entities involved in claims processing—health care providers, health plans, and health clearinghouses. Under the HIPAA Privacy Rule, protected health information may lose its protection after it travels from a covered entity to a noncovered entity. By contrast, the NHIN is designed to develop an interoperable infrastructure for coordinated, secure, personal exchange. The NHIN has a much broader scope and therefore, privacy and confidentiality rules must apply more broadly than is currently the case under the HIPAA Privacy Rule.

Recommendations on jurisdiction, scope, and relationships with other laws:

I-12. HHS should work with other federal agencies and the Congress to ensure 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.[3]

I-13. HHS should explore ways to preserve some degree of state variation in health privacy law without losing systemic interoperability and essential protections for privacy and confidentiality.

I-14. HHS should harmonize the rules governing the NHIN with the HIPAA Privacy Rule, as well as other relevant federal regulations, including those regulating substance abuse treatment records.

Procedures

The NHIN would create a structure for disclosing sensitive information that previously was primarily controlled locally by health care professionals and health care administrators. Because the NHIN would represent a substantial change from current health information practices, the process of creating, implementing, and administering the NHIN must be open and transparent. HHS should encourage the input and participation of a broad cross-section of the population. The creation of the American Health Information Community (AHIC) is a valuable step in this direction. NCVHS will, in open and public sessions this summer, be reviewing an initial set of functional requirements for NHIN services.[4] However, to ensure success, there is a continued need for regular, meaningful participation in the design and implementation of the NHIN by organizations, groups, and individuals affected by its creation. This participation must include members of medically vulnerable and minority populations.

Fair information practices should be incorporated into the NHIN. Some examples include the right to see an accounting of disclosures of one's record, the right to correct errors, and the right to a procedure for redress—investigation and resolution of complaints filed by individuals. An important information practice that has received significant attention in the press in the last year is how the system responds to incidents of unauthorized access to identifiable information, and whether the subjects of the unauthorized disclosure should be notified when the breach is discovered. That issue is very important to establishing the trust in the system, but NCVHS has decided not to address the issue now, so that the specifics can be addressed in a separate letter dealing with security issues more broadly.

Recommendations on procedures:

I-15. HHS should incorporate fair information practices into the architecture of the NHIN.

I-16. HHS should use an open, transparent, and public process for developing the rules applicable to the NHIN, and it should solicit the active participation of affected individuals, groups, and organizations, including medically vulnerable and minority populations.

[3] See the Committee's June 2007 letter on Recommendation 12 (page 21).
[4] NCVHS Functional Requirements recommendation—http://www.ncvhs.hhs.gov/061030lt.pdf.

Enforcement

Several witnesses testified that strong enforcement and meaningful penalties are essential to deter wrongdoing and to assure the public that breaches of privacy, confidentiality, or security are taken seriously and will be dealt with aggressively. We believe that appropriate civil and criminal sanctions should be imposed on individuals and entities responsible for the violation of confidentiality and security provisions of EHRs and the NHIN. Under the HIPAA Privacy Rule, enforcement is in the hands of the Secretary, and an individual who is aggrieved must file a complaint with the Department to obtain relief under federal law. There is no private right of action. The Office for Civil Rights attempts to resolve those problems that lead to complaints directly with the covered entities, and we applaud the focus on improving the protections at the covered entity level. Nonetheless, prospective, general improvements by a covered entity often do not satisfy the individual who makes the complaint nor reassure the public that the law is being enforced adequately. A commitment to aggressive enforcement on the part of federal regulators is necessary to ensure the adoption and success of the NHIN.

There are many choices as to enforcement mechanisms that might be appropriate for the NHIN, including civil fines, revocation of licenses, withdrawal of membership rights, suspension or termination from participation in Medicare or Medicaid, payment of restitution, private rights of action, and criminal sanctions. These enforcement mechanisms might be imposed by legislation, regulation, contractual agreements, self-regulatory authorities, certifying or licensing boards, or other approaches. In the special case of unauthorized uses or disclosures in foreign jurisdictions, additional enforcement mechanisms might include international agreements on the protection of personal health information transmitted across national boundaries, limitations on the transmission of such information outside of the United States, or special licensing and registration requirements for foreign business associates. The success of the NHIN will depend on finding an appropriate suite of measures that produces high levels of compliance on the part of the custodians of individually identifiable information, but does not impose a level of complexity or cost that discourages investment.

NCVHS believes that, to date, the focus of the Department has been largely on developing infrastructure and generating investment. While both are critical, the Department should not neglect the policies and procedures that will control creation, collection, maintenance, use, disclosure, and eventual disposition of the information. A high level of enforcement is necessary to establish public confidence that privacy and confidentiality are properly protected. The NHIN also requires the widespread belief that its system of redress is responsive and fair. These policies cannot be created after the network is in place—by then it will be too late to impose new policies on an existing infrastructure. The policies must be built into the architecture from the beginning.

Among the enforcement principles for inclusion in the NHIN are the following: a wide range of penalties and sanctions should be available; penalties should be progressive, with the most severe ones for willful and knowing violations, repeat offenders, or egregious wrongs; individuals should be entitled to some remedy for unlawful dis-

closures, including compensation for actual harm; establishing a new, federal private right of action should be avoided; and alternative dispute resolution should be encouraged.

Recommendations on enforcement:

I-17. *HHS should develop a set of strong enforcement measures that produces high levels of compliance with the rules applicable to the NHIN on the part of custodians of personal health information, but does not impose an excessive level of complexity or cost.*

I-18. *HHS should ensure that policies requiring a high level of compliance are built into the architecture of the NHIN.*

I-19. *HHS should adopt a rule providing that continued participation in the NHIN by an organization is contingent on compliance with the NHIN's privacy, confidentiality, and security rules.*

I-20. *HHS should ensure that appropriate penalties be imposed for egregious privacy, confidentiality, or security violations committed by any individual or entity.*

I-21. *HHS should seek to ensure through legislative, regulatory, or other means that individuals whose privacy, confidentiality, or security is breached are entitled to reasonable compensation.*

F. Secondary Uses[5]

Many individuals are concerned about the disclosure of their confidential personal health information because of possible embarrassment, emotional distress, and stigma. They are also concerned about more tangible harms, such as the inability to obtain employment, mortgages and other loans, or various forms of insurance. Measures to protect the security of personal health information from unauthorized access and to protect the confidentiality of disclosures through fair information practices are extremely important. Nonetheless, these measures will only have a limited effect in addressing the public's primary concern about health "privacy"—the use of personal health information to adversely affect individuals' personal, financial and professional rights, interests, and opportunities.

Limitation on uses by third parties

In Section D, we discussed the importance of building into the architecture of the NHIN the capacity to use contextual access criteria to limit the scope of personal health information when disclosure is made to third parties pursuant to an authorization. The ability of holders of personal health information to limit disclosures to relevant information solves only part of the problem. Third party users of personal health information should be restricted to requiring authorization only for relevant personal health information. Furthermore, any personal health information obtained by a third party in a context outside of the healthcare system should not be used unfairly to adversely affect an individual's personal, financial, or professional rights, interests, or opportunities.

[5] See NCVHS, Enhancing Protections for Uses of Health Data: A Stewardship Framework. Full report, December 2007; Summary for Policy Makers. April 2008.

All of these elements are essential to meaningful protection of individual privacy. Without information technology capable of protecting information from inappropriate disclosures, restricting access or use by third parties will be meaningless and without practical effect. At the same time, without appropriate restrictions to prevent third parties from obtaining or using personal health information in a context incompatible with individuals' expectations of appropriate use of their personal health information, third parties could evade the contextual access criteria of EHRs and the NHIN by simply demanding that individuals provide copies of records at the time of application for employment, loans, or insurance. Undoubtedly, the more often personal health information is available in a context outside of healthcare delivery, the more likely individuals will be unfairly discriminated against. NCVHS urges the Secretary to pursue legislative or regulatory measures designed to eliminate or reduce as much as possible the potential discriminatory effects of personal health information disclosures beyond health care.

Recommendation on uses by third parties:

I-22. HHS should support legislative or regulatory measures to eliminate or reduce as much as possible the potential harmful discriminatory effects of personal health information disclosure.

Relationship to the HIPAA Privacy Rule

More effective control of personal health information will require reconsideration of several key provisions of the HIPAA Privacy Rule. For example, under the current Privacy Rule, covered entities have limited responsibilities and limited recourse in oversight of the privacy and confidentiality procedures of business associates. When the Privacy Rule was promulgated, HHS recognized the business associate relationship and imposed some limitations to protect the privacy of financial transactions, but the current rule is inadequate to deal with relationships in which personal health information is shared directly between covered entities and their business associates. If the Privacy Rule is not amended, the new system of EHRs and the NHIN would permit domestic and overseas business associates to be able to obtain much more personal health information without any more oversight. Indeed, in the case of overseas associateships, which are increasing in the commercial marketplace, understanding or controlling the use of information may be particularly difficult.

Another area of concern involves the redisclosure of personal health information obtained by third parties pursuant to an authorization. Once information has been obtained by the commercial entity, it is not protected by the Privacy Rule. These and similar issues have been addressed in prior recommendations by NCVHS,[6] and the more comprehensive disclosures via the NHIN make action on these recommendations imperative.

[6] See NCVHS September 2004 letter on effect of the Privacy Rule—http://www.ncvhs.hhs.gov/040901lt1.htm.

The HIPAA Privacy Rule was based on a "chain of trust" model, permitting information to flow freely among those involved directly in treatment, payment, or health care operations. However, an interoperable information sharing environment for personal health information will increase the amount of information that can flow to parties not originally contemplated by the Privacy Rule, that is, those outside of the realm of treatment, payment, and health care operations. As information flows away from the people and organizations that collect and use it for its primary purpose, health care delivery, it becomes increasingly difficult to understand or control how it is being used for secondary or even tertiary purposes. Therefore, before moving to the NHIN, it is essential to tighten the gaps in the Privacy Rule that permit information to leak and to adopt a more comprehensive privacy protection regime.

Recommendation on relationship to the HIPAA Privacy Rule:

I-23. NCVHS endorses strong enforcement of the HIPAA Privacy Rule with regard to business associates, and, if necessary, HHS should amend the Rule to increase the responsibility of covered entities to control the privacy, confidentiality, and security practices of business associates.

G. Establishing and Maintaining Public Trust

NCVHS heard testimony that Americans are unsure whether the benefits of an NHIN outweigh the privacy risks, concerned about security of their information, and lacking in confidence about federal regulation. NCVHS observed that members of the public lack knowledge and understanding about what records exist about them, how they are used and shared, and what rules apply. There are also few opportunities for public participation in developing national health information policy. Consequently, public trust is lacking as we develop the NHIN.

The public concerns about EHRs and the NHIN make it essential that HHS and other public and private entities begin immediate, substantial, and sustained efforts to establish and maintain public trust in the NHIN. Maintaining a high level of public trust must be a key consideration of all associated with developing the NHIN. HHS must pursue three simultaneous courses to succeed at this goal. First, HHS must ensure that individuals understand what they stand to gain with the advent of the NHIN, and receive a fair assessment of the risks. At a time when media reports are much more likely to focus on rare security breaches than the everyday health benefits of EHRs, a major effort in public and professional education is essential. The NHIN cannot be imposed on the public; the public must be informed about the NHIN's weaknesses and strengths, risks and benefits, and become convinced of its merits.

What will convince the public? NCVHS finds that the one benefit that will win over public support is better health care. If we expect individuals to support an interoperable network

that permits quick and easy data sharing, the indispensable requisite must be a measurable improvement in the quality of individual care. During our hearings on the NHIN, one witness suggested that for its first 5 years of operation, the NHIN should be used exclusively for patient care, and only after public trust in the system is established would the system be available for quality assurance, outcomes research, syndromic surveillance, and other purposes. Some have even suggested that individual health care is so important that it should be *the only* purpose for which information can ever be used. These suggestions make it clear that the individual health care benefits of the NHIN must be the top priority of developers, and must be the centerpiece of public education programs. Individuals are typically willing to disclose information and absorb some risk to privacy if they get some direct personal benefit in return, but general improvements in quality assurance, outcomes research, decision support, and public health, or other diffuse societal benefits, are unlikely to persuade individuals to undertake the personal risk of making their own information health available over the NHIN. The focus of the NHIN developers and any public education efforts must be on direct, individual benefits and improving individual care.

Second, meaningful input and participation will help improve understanding of the system and increase the public's level of comfort that the NHIN's benefits outweigh its risks. We have previously indicated the importance of public participation in the design, functioning, and oversight of the NHIN. We also stressed the importance of carefully crafted regulatory procedures and enforcement authority. These "substantive" measures will help to instill public confidence in the operation of the system. In addition, AHIC and other groups should take special care in ensuring that the public is thoroughly and thoughtfully engaged in the development and oversight of the NHIN.

Third, HHS must establish an ongoing program of measuring and assessing the effectiveness of the privacy and confidentiality protections of the NHIN and the level of individual understanding and public confidence in those protections. NCVHS believes that the NHIN will have greater credibility, and public trust will be enhanced if this research, at least initially, is undertaken by independent investigators who are contractors or grantees of HHS than if the review is performed internally by HHS.

Recommendations on establishing and maintaining public trust:

I-24. Public and professional education should be a top priority for HHS and all other entities of the NHIN.

I-25. Meaningful numbers of consumers should be appointed to serve on all national, regional, and local boards governing the NHIN.

I-26. HHS should establish and support ongoing research to assess the effectiveness and public confidence in the privacy, confidentiality, and security of the NHIN and its components.

June 2007: A Call for a More Comprehensive Federal Privacy Law

Following the June 2006 letter-report, the Subcommittee on Privacy and Confidentiality held three hearings to learn about the health privacy practices of entities that make significant use of health information but are not covered by the HIPAA Privacy Rule.

The testimony in these hearings reinforced the Committee's conviction that all entities that deal with personally identifiable health information should be covered by some federal privacy law. With that standard in mind, the Subcommittee identified the following issues:

- Many entities that may play key roles in the NHIN (e.g., those responsible for data storage or transit) may fall outside HIPAA's statutory definition of covered entity and also may not qualify as clearinghouses or have entered into business associate agreements.
- A significant number of everyday providers of health care and health-related services are not covered by HIPAA. This includes (1) providers that do not submit claims for payment in electronic form; (2) providers that are directly paid by their customers or another party (e.g., massage therapists, nutritional counselors, and urgent care facilities); and (3) providers that create records covered by the Family Educational Rights and Privacy Act (FERPA), who are excluded from the HIPAA definition of protected health information.

II. Update to Privacy Laws and Regulations Required To Accommodate Nationwide Health Information Network Data Sharing Practices

June 21, 2007

The present communication follows up on the National Committee's June 22, 2006, letter report, Privacy and Confidentiality in the Nationwide Health Information Network. Among the 26 recommendations was the following:

> I-12. HHS should work with other federal agencies and the Congress to ensure 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.

NCVHS held a series of three hearings in 2006-2007 to learn more about the health privacy practices of entities that make significant use of health information in their day-to-day operations but are not covered by the Health Insurance Portability and Accountability Act (HIPAA). At the first two hearings, we heard from representatives of life insurers, insurance regulators, human resource professionals, occupational health physicians, financial institutions, primary and secondary schools, and colleges. The third hearing focused on health care providers and other entities in the health industry that are not covered by the HIPAA privacy rule. We inquired about the degree to which they are regulated by other federal or state laws and the possible effects that federal health privacy coverage would have on their operations.

What we learned from the testimony strongly reinforces our conviction that all entities that deal with personally identifiable health information should be covered by some federal privacy law. NCVHS would like to share some additional observations in support of our earlier recommendation with respect to this last group of noncovered entities, those operating in the health care arena.

A significant concern is that many of the new entities essential to the operation of the Nationwide Health Information Network (NHIN) fall outside HIPAA's statutory definition of "covered entity." Health information exchanges, regional health information organizations, record locator services, community access services, system integrators, medical record banks, and other new entities established to manage health information have proliferated in recent years. While some of these entities may be business associates under the Privacy Rule, and thus obligated by contractual agreements with covered entities to maintain similar standards, others may not be business associates. Moreover, it is the view of NCVHS that business associate arrangements are not sufficiently robust to protect the privacy and security of all individually identifiable health information. Business associates are subject only to contract claims brought by the covered entity and not to enforcement actions by HHS or the Department of Justice. The health information technology community is moving quickly in response to the Department's efforts on the NHIN, but our hearings have revealed that, even today, numerous

individually identifiable health records are not subject to federal privacy and security protections. This remarkable fact underscores our view that all individually identifiable health information created, collected, stored, or transmitted should enjoy the protections of a federal privacy standard.

In addition to new entities that manage health information, mentioned previously, NCVHS also heard from representatives of noncovered healthcare providers: the National Athletic Trainers' Association, the International Medical Spa Association, a large employer participating in a multi-employer personal health record system, a health record bank organization, and a home testing laboratory. We also heard from legal experts who addressed various issues associated with these entities, such as the status of medical practices that operate on a cash only basis and the disposition of the health records of entities that enter into bankruptcy.

Based on the testimony we heard, we now understand that a significant number of everyday providers of health care and health-related services are not covered by the HIPAA privacy and security rules. These entities fall into two categories. In the first category are entities that do not submit claims for payment in electronic form. These entities are not covered because the definition of a covered provider is connected to the original purpose of HIPAA—administrative simplification of the processing of claims. Since these entities do not submit claims or bill health plans electronically, they fall outside the definition and are not covered. Among the health care providers not covered by HIPAA are entities that are directly paid by their customers or another party, such as some of the following providers: cosmetic medicine services, occupational health clinics, fitness clubs, home testing laboratories, massage therapists, nutritional counselors, "alternative" medicine practitioners, and urgent care facilities.

In the second category are providers that create records covered by the Family Educational Rights and Privacy Act (FERPA), which are explicitly excluded from the definition of "protected health information" in the HIPAA Privacy Rule. FERPA, which is overseen by the Department of Education, protects records of students in schools that receive Department of Education funds. Thus, most health records created and maintained by school clinics falls under FERPA rather than HIPAA. However, some schools are not covered by either law. Some providers, such as athletic trainers working in scholastic athletic programs, or college student health services that submit electronic insurance claims, have reported confusion as to whether they are subject to HIPAA or to FERPA. Today, under separate cover, we are also sending a letter addressing this matter.[7]

The HIPAA privacy and security rules were designed to set minimum, uniform protections for identifiable health information across the nation. Providers of health care and related services not subject to HIPAA may also not be subject to any other state or federal privacy law. This means they may be free to engage in a wide range of practices otherwise not permitted under HIPAA. For example, noncovered entities are not required to provide notices to individuals about their privacy practices, train their staffs about privacy and confidentiality, institute physical controls on the storage or use of health records, protect electronic transmissions of health information, maintain an accounting

[7] See the June 21, 2007, NCVHS letter on "Improving the interaction of FERPA and the HIPAA Privacy Rule with regard to school health records," posted on the NCVHS website.

of disclosures, or require an authorization before redisclosing health information to other noncovered entities. These entities may even sell personal health information without authorization for the purpose of marketing or other purposes that consumers may find objectionable.

In the context of the NHIN, it will be easier to design health information products and services with knowledge of privacy requirements than to retrofit them to new privacy policies. Therefore, time is of the essence.

Recommendation on ensuring comprehensive privacy protections:

II-1. HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.

February 2008: Recommendations on Individual Control of Sensitive Health Information

The Subcommittee on Privacy and Confidentiality further investigated recommendations I-6 and I-7 from the June 2006 letter (regarding individual control of sensitive health information). Through extensive deliberation with the full NCVHS, a letter-report discussing individual control of sensitive health information was submitted in February 2008. The report stated that "individual control of sensitive health information is one of the most important privacy issues to be resolved in developing and implementing the NHIN." The report also stressed the urgency of these "complicated, contentious, and crucial" issues and offered the Committee's continued active involvement.

The report made the following recommendations to the Secretary:

- The Secretary should adopt a policy for the NHIN to allow individuals to have limited control, in a uniform manner, over the disclosure of certain sensitive health information for purposes of treatment. (The letter-report does not address questions about individual control over disclosures for other purposes such as quality, billing, and research.)
- Public dialogue is needed to develop the specifics of policies on individual control, and implementation of the policies should be pilot tested.
- Sequestering information in sensitive categories is a reasonable solution to the need to protect the confidentiality of certain information. (The Committee reached this conclusion after considering a range of options that are explained in the letter report.)
- NCVHS also put forward recommendations on provider notification, emergency access, resequestration, clinical decision support, and research.

III. Individual Control of Sensitive Health Information Accessible via the Nationwide Health Information Network for Purposes of Treatment

February 20, 2008

Individual control of sensitive health information accessible via the Nationwide Health Information Network (NHIN) is a matter of great concern to patients, practitioners, insurers, policymakers, and others, and there is no federal law or policy that specifically addresses this issue. Over the course of 4 years, the National Committee on Vital and Health Statistics (NCVHS) has deliberated extensively about how best to ensure that appropriate privacy protections are included in the emerging NHIN. With the increasing adoption of electronic health information networks in the public and private sectors and development of the NHIN, it is imperative to address this matter now.

This letter recommends that the Secretary adopt a policy for the NHIN to allow individuals to have limited 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 NCVHS.

On June 22, 2006, NCVHS sent the Secretary a letter report, Privacy and Confidentiality in the Nationwide Health Information Network.[8] Among the 26 recommendations were the following:

> I-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.*
>
> I-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.*

[8] Pages 3–19 in this monograph.

In an effort to provide 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.

A. 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 United States 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.

B. 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 in the following text. 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 in the following text 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, socioeconomic 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, professional and accreditation standards, and requirements. NCVHS believes that a public process for addressing these issues is essential.

Example categories:

- Domestic violence
- Genetic information
- Mental health information
- Reproductive health
- Substance abuse

Through testimony and Committee discussion, legitimate concerns were raised about how sequestering categories of health information could affect medical malpractice liability. Liability could potentially be affected in at least two ways. The sequestration of critical information might cause providers to give less than optimal advice or treatment because critical information is not considered. 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.

C. 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 seques-

tered 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.

D. Emergency Access

In an emergency where a patient is unable to give or refuse consent to access sequestered health information, including when an unconscious, delirious, or otherwise incompetent patient is treated in an emergency department, physician's office, or other health care setting, it may be extremely beneficial 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 the relevant privacy officer. 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.

E. Resequestration 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 on sequestration:

III-1. This 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:

a. 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 on a national basis so that it is uniform across the NHIN.

b. 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.

c. The design of the NHIN should ensure that when a health care provider accesses health information with one or more categories sequestered, a notation indicates that sensitive health information has been sequestered at the direction of the patient. The specificity of the notation will need to be determined.

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

e. The design of 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.

f. The design of the NHIN should provide that if a health care provider obtains emergency access to sequestered information, a description of the circumstances surrounding access are made part of the audit trail, and the health care entity's designated privacy official is notified automatically.

g. The design of the NHIN should provide that if a health care provider obtains emergency access to sequestered health information, the patient or the patient's representative is notified promptly.

h. 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.

F. Other Options the National Committee on Vital Health Statistics Considered

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

No sharing restrictions. One possibility would be 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 nonsensitive 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, nonemergency 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.

G. 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 on clinical decision support:

III-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.

H. 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 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.

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.

Recommendations on research, development, and implementation:

III-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.

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

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

Appendix I.

National Committee on Vital and Health Statistics Recommendations on Privacy and Confidentiality, 2006–2008

I. Privacy and Confidentiality in the Nationwide Health Information Network (June 2006)

Recommendation on flexibility or uniformity:

I-1. *The method by which personal health information is stored by health care providers should be left to the health care providers.*

Recommendations on mandatory or voluntary participation:

I-2. *Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN.*

I-3. *Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN.*

I-4. *HHS should monitor the development of opt-in/opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social, and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate.*

I-5. *HHS should require that individuals be provided with understandable and culturally sensitive information and education to ensure that they realize the implications of their decisions as to whether to participate in the NHIN.*

Recommendations on individual control:[9]

I-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.*

I-7. *If individuals are given the 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.*

Recommendations on disclosure:

I-8. *Role-based access should be employed as a means to limit the personal health information accessible via the NHIN and its components.*

I-9. *HHS should investigate the feasibility of applying contextual access criteria to EHRs and the NHIN, enabling personal information disclosed beyond the health care setting on the basis of an authorization to be limited to the information reasonably necessary to achieve the purpose of the disclosure.*

I-10. *HHS should support research and technology to develop contextual access criteria appropriate for application to EHRs and inclusion in the architecture of the NHIN.*

[9]See the NCVHS February 2008 recommendations on individual control, page 10

I-11. HHS should convene or support efforts to convene a diversity of interested parties to design, define, and develop role-based access criteria and contextual access criteria appropriate for application to EHRs and the NHIN.

Recommendations on jurisdiction, scope, and relationships with other laws:

I-12. HHS should work with other federal agencies and the Congress to ensure 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.

I-13. HHS should explore ways to preserve some degree of state variation in health privacy law without losing systemic interoperability and essential protections for privacy and confidentiality.

I-14. HHS should harmonize the rules governing the NHIN with the HIPAA Privacy Rule, as well as other relevant federal regulations, including those regulating substance abuse treatment records.

Recommendations on procedures:

I-15. HHS should incorporate fair information practices into the architecture of the NHIN.

I-16. HHS should use an open, transparent, and public process for developing the rules applicable to the NHIN, and it should solicit the active participation of affected individuals, groups, and organizations, including medically vulnerable and minority populations.

Recommendations on enforcement:

I-17. HHS should develop a set of strong enforcement measures that produces high levels of compliance with the rules applicable to the NHIN on the part of custodians of personal health information, but does not impose an excessive level of complexity or cost.

I-18. HHS should ensure that policies requiring a high level of compliance are built into the architecture of the NHIN.

I-19. HHS should adopt a rule providing that continued participation in the NHIN by an organization is contingent on compliance with the NHIN's privacy, confidentiality, and security rules.

I-20. HHS should ensure that appropriate penalties be imposed for egregious privacy, confidentiality, or security violations committed by any individual or entity.

I-21. HHS should seek to ensure through legislative, regulatory, or other means that individuals whose privacy, confidentiality, or security is breached are entitled to reasonable compensation.

Recommendation on uses by third parties:

I-22. HHS should support legislative or regulatory measures to eliminate or reduce as much as possible the potential harmful discriminatory effects of personal health information disclosure.

Recommendation on relationship to the HIPAA Privacy Rule:

I-23. NCVHS endorses strong enforcement of the HIPAA Privacy Rule with regard to business associates, and, if necessary, HHS should amend the Rule to increase the responsibility of covered entities to control the privacy, confidentiality, and security practices of business associates.

Recommendations on establishing and maintaining public trust:

I-24. Public and professional education should be a top priority for HHS and all other entities of the NHIN.

I-25. Meaningful numbers of consumers should be appointed to serve on all national, regional, and local boards governing the NHIN.

I-26. HHS should establish and support ongoing research to assess the effectiveness and public confidence in the privacy, confidentiality, and security of the NHIN and its components.

II. Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices (June 2007)

Recommendation on ensuring comprehensive privacy protections:

II-1. HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.

III. Individual Control of Sensitive Health Information Accessible via the Nationwide Health Information Network for Purposes of Treatment

Recommendations on sequestration:

III-1. This 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:

a. 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 on a national basis so that it is uniform across the NHIN.

b. 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.

c. The design of the NHIN should ensure that when a health care provider accesses health information with one or more categories sequestered, a notation indicates that sensitive health information has been sequestered at the direction of the patient. The specificity of the notation will need to be determined.

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

e. The design of 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.

f. The design of the NHIN should provide that if a health care provider obtains emergency access to sequestered information, a description of the circumstances surrounding access are made part of the audit trail, and the health care entity's designated privacy official is notified automatically.

g. The design of the NHIN should provide that if a health care provider obtains emergency access to sequestered health information, the patient or the patient's representative is notified promptly.

h. 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.

Recommendation on clinical decision support:

III-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.

Recommendations on research, development, and implementation:

III-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.

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

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

During this period, NCVHS also issued other recommendations relevant to health information privacy and confidentiality that were developed by other NCVHS subcommittees and workgroups:

- Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network (October 2006)
- Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data (December 2007)
- Enhancing Protections for Uses of Health Data: A Stewardship Framework: Summary for Policy Makers (April 2008)

All NCVHS letters, reports, and letter reports are posted on its website, http://www.ncvhs.dhhs.gov.

Appendix II.

National Committee on Vital and Health Statistics Full Committee and Subcommittee on Privacy Members, 2006–2008

Chairman

Simon P. Cohn, M.D., M.P.H. * **
Associate Executive Director
The Permanente Federation
Kaiser Permanente
Oakland, CA 94612

HHS Executive Staff Director

James Scanlon
Deputy Assistant Secretary
Office of Science and Data Policy
Office of the Assistant Secretary
for Planning and Evaluation, HHS
Washington, DC 20201

Executive Secretary

Marjorie S. Greenberg
Chief, Classifications and Public Health Data
Standards Staff
Office of the Director
National Center for Health Statistics
Centers for Disease Control and Prevention
Hyattsville, MD 20782

Membership

Jeffrey S. Blair, M.B.A.
Director of Health Informatics
Lovelace Clinic Foundation
Albuquerque, NM 87106

Justine M. Carr, M.D.
Chief Medical Officer
Senior Vice President for Quality, Safety, and
Medical Affairs
Caritas Christi Healthcare
Boston, MA 02135

Leslie Pickering Francis, J.D., Ph.D.*
Chairman, Department of Philosophy
Alfred C. Emery Professor of Law
University of Utah
Salt Lake City, UT 84112

Larry A. Green, M.D.
University of Colorado
Department of Family Medicine
Health Science Center
Aurora, CO 80045

John P. Houston, J.D.*
Vice President, Privacy and Information
Security Assistant Counsel and Adjunct
Assistant Professor of Biomedical Informatics
University of Pittsburgh School of Medicine
Pittsburgh, PA 15213

Garland Land, M.P.H.
Executive Director
National Association for Public Health
Statistics and Information Systems
Silver Spring, MD 20910

*Members of the Privacy and Security Subcommittee, 2006–2008.
**Members retired in 2008.

Carol J. McCall, F.S.A., M.A.A.A.
Vice President
Humana
Center for Health Metrics
Louisville, KY 40202

J. Marc Overhage, M.D., Ph.D.
President and CEO
Indiana Health Information Exchange
Associate Professor, Indiana University School Of Medicine
Senior Research Scientist, Regenstrief Institute
Regenstrief Institute, Inc.
Indianapolis, IN 46202

Harry Reynolds*
Vice President
Blue Cross Blue Shield of North Carolina
Durham, NC 27702

Mark A. Rothstein, J.D. ** ***
Herbert F. Boehl Chair of Law and Medicine
Director, Institute for Bioethics, Health Policy, and Law
University of Louisville School of Medicine
Louisville, KY 40292

William J. Scanlon, Ph.D.
Health Policy R&D
Washington, DC 20001

Donald M. Steinwachs, Ph.D.
Interim Provost
Senior Vice President for Academic Affairs
The Johns Hopkins University
Bloomberg School of Public Health
Department of Health Policy and Management
Health Services Research and Development Center
Baltimore, MD 21205

C. Eugene Steuerle, Ph.D. **
Senior Fellow
The Urban Institute
Washington, DC 20037

Paul Tang, M.D.*
Chief Medical Information Officer
Palo Alto Medical Foundation
Palo Alto, CA 94301

Kevin C. Vigilante, M.D., M.P.H.**
Principal
Booz-Allen & Hamilton
Rockville, MD 20852

Judith Warren, Ph.D., R.N.
Christine A. Hartley Centennial Professor
Director of Nursing Informatics, KUMC Center for Healthcare Informatics
University of Kansas School of Nursing
Kansas City, KS 66160

*Members of the Privacy and Security Subcommittee, 2006–2008.
**Members retired in 2008.
***Chairman, NCVHS Subcommittee on Privacy and Security, 2006–2008.

Liaison Representatives

J. Michael Fitzmaurice, Ph.D.
Senior Science Advisor for Information Technology
Agency for Healthcare Research and Quality
Rockville, MD 20850

Edward J. Sondik, Ph.D.
Director
National Center for Health Statistics
Hyattsville, MD 20782

Karen Trudel
Deputy Director
Office of E-Health Standards and Services
Centers for Medicare and Medicaid Services
Baltimore, MD 21244

Jim Lepkowski, Ph.D.
Institute for Social Research
University of Michigan
Ann Arbor, MI 48104

Steven J. Steindel, Ph.D.
Senior Advisor
Standards and Vocabulary Resource
Information Resources Management Office
Centers for Disease Control and Prevention
Atlanta, GA 30333

NCVHS Members Added in 2008

Mark C. Hornbrook, Ph.D.
Chief Scientist
The Center for Health Research Northwest-Hawaii-Southeast
Kaiser Permanente Northwest
Portland, OR 97227

Sallie Milam, J.D.
Executive Director
West Virginia Health Information Network
Chief Privacy Officer
West Virginia State Government
Charleston, WV 25311

Blackford Middleton, M.D., M.P.H., 0-.
Corporate Director, Clinical Informatics Research and Development
Chairman, Center for Information Technology Partners Healthcare
Wellesley, MA 02481

Walter G. Suarez, M.D., M.P.H.
President and CEO
Institute for HIPAA/HIT Education and Research
514 Triadelphia Way
Alexandria, VA 22312

Maya Bernstein, J.D., served as lead staff for the Privacy Subcommittee.
Susan Baird Kanaan, writer for NCVHS, assisted in preparation of this monograph.
Current NCVHS membership may be found on http://www.ncvhs.dhhs.gov.

CS200708
T33852 (5/2009)