June 22, 2006

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

Dear Secretary Leavitt:

I am pleased to present you with a report of the National Committee on Vital and Health Statistics recommending actions regarding "Privacy and Confidentiality in the Nationwide Health Information Network." This report and its recommendations are the culmination of an 18 month process of learning and deliberation. The Subcommittee on Privacy and Confidentiality held three hearings in Washington, D.C., one in Chicago, and one in San Francisco. At each hearing, witnesses representing different constituencies concerned about the privacy and confidentiality of health information testified, 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 hearings were followed by a series of conference calls and public meetings to discuss findings and prepare this report for the Committee to submit to HHS. Several times the Subcommittee presented its progress to the Committee and invited questions and comments. A thorough and animated discussion of the report at the full Committee meeting earlier this month culminated in approval.

The report covers several topics central to the challenges for safeguarding health privacy in the NHIN environment: 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 non-health care entities, and establishing and maintaining the public trust that is necessary to ensure NHIN is a success. We hope that our analysis and recommendations will be valuable as the Department considers these important issues.

In presenting this report, the NCVHS acknowledges that the broad contour of the NHIN is still being determined. We will continue to update and refine these recommendations as the architecture and functional requirements of the NHIN advance.

We appreciate the opportunity to play a role in helping to shape the nation's health information policy.
.

Sincerely,

/s/

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

Cc: Data Council Co-chairs
Enclosures

PRIVACY AND CONFIDENTIALITY IN THE NATIONWIDE HEALTH INFORMATION NETWORK

The Nationwide Health Information Network (NHIN), on which the 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 the 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.

The 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 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 the 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. 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.

1. 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. The 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

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

2. Mandatory or voluntary participation?

The next issue to consider is whether participation in the NHIN should be mandatory. The 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 the 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

R-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.

R-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.

R-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.

R-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.

3. What is 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 we describe below the arguments that the 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.

4. The degree of 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.

5. 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 the 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 C.3. above.

The NCVHS heard testimony from experts about the Australian, British, Canadian, and Danish health systems, which 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

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

R-7 If individuals are given 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.

<u>Recommendations</u>

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

R-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.

R-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.

R-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.

1. 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 non-covered 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

R-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.

R-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.

R-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.

2. 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. 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 the 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.

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

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

Recommendations

R-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. .

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

R-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.

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

R-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

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.

1. 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.

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

R-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.

2. 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 the NCVHS, and the more comprehensive disclosures via the NHIN make action on these recommendations imperative.

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, i.e., 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

R-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

The 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 five 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. The 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

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

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

R-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.